HR940

Authorizations in SAP ERP HCM

PARTICIPANT HANDBOOK
INSTRUCTOR-LED TRAINING

Course Version: 2108
Course Duration: 4 Day(s)
Material Number: 50157804

SAP Copyrights, Trademarks and Disclaimers

Typographic Conventions

American English is the standard used in this handbook.

The following typographic conventions are also used.

This information is displayed in the instructor's presentation	
Demonstration	
Procedure	
Warning or Caution	
Hint	
Related or Additional Information	
Facilitated Discussion	
User interface control	*Example text*
Window title	*Example text*

Contents

Course Overview

TARGET AUDIENCE

This course is intended for the following audiences:

- Data Manager
- Application Consultant
- Data Consultant
- Business Process Owner/Team Lead/Power User

UNIT 1 HCM Authorization Basics

UNIT OBJECTIVES

- Outline HCM authorization types
- Outline the general authorization check
- Outline the structural authorization check
- Create a user master record for an existing employee
- Copy sample roles delivered by SAP

Unit 1
Lesson 1

Outlining HCM Authorizations

LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Outline HCM authorization types
- Outline the general authorization check
- Outline the structural authorization check

HCM Authorization Types

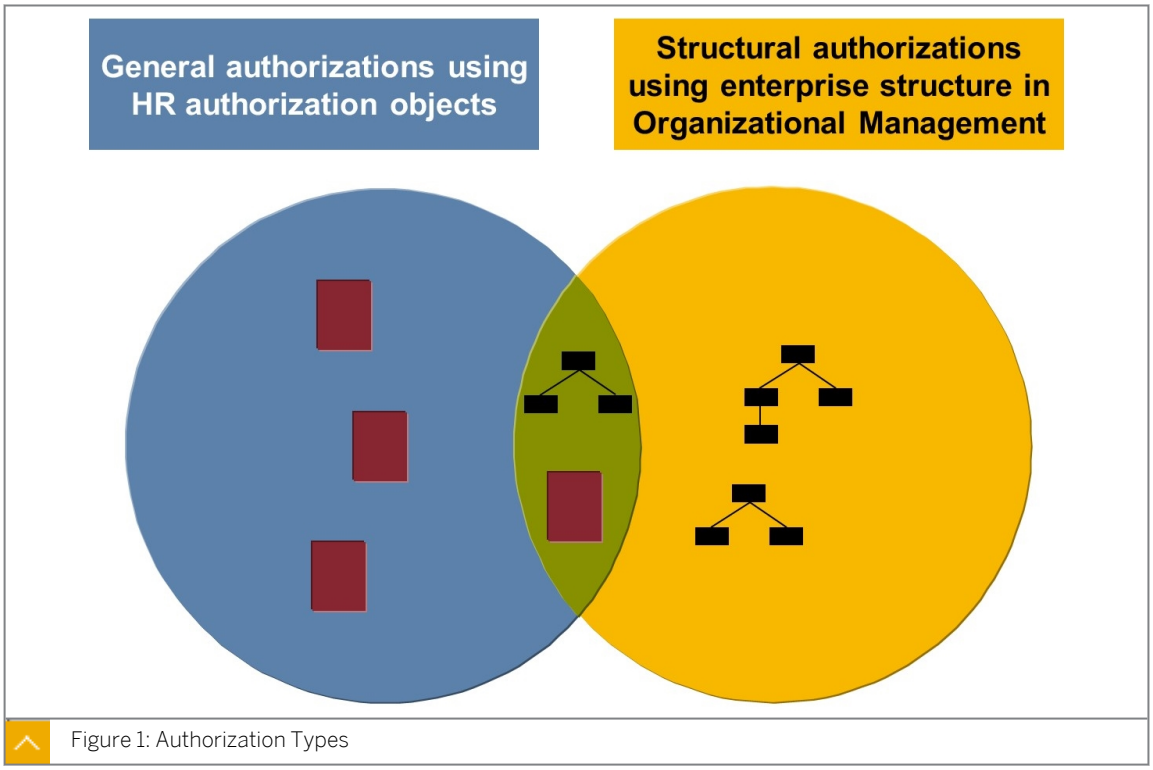

Figure 1: Authorization Types

An authorization check is a method by which the system controls a user's access to system data. Assigning authorizations is a fundamental prerequisite for the implementation of business software so that only authorized users access specific data. In SAP HCM, you can set up two types of authorizations, general and structural.

The following are the two main authorizations you can set up in HCM:

- General authorizations

It is mandatory to create general authorizations for your organization. The general authorizations include the authorizations that are necessary for Personnel Administration and that help control access to HR data. This HR data must be strictly controlled due to its sensitive nature.

- Structural authorizations

  It is optional to set up HCM specific structural authorizations. Structural authorizations check, by organizational assignment, if a user is authorized to perform an activity. If you want to use structural authorizations, you must map your enterprise's structure in Organizational Management.

You can simultaneously set up both general and structural authorization types to achieve a complex authorization concept.

General Authorization Check

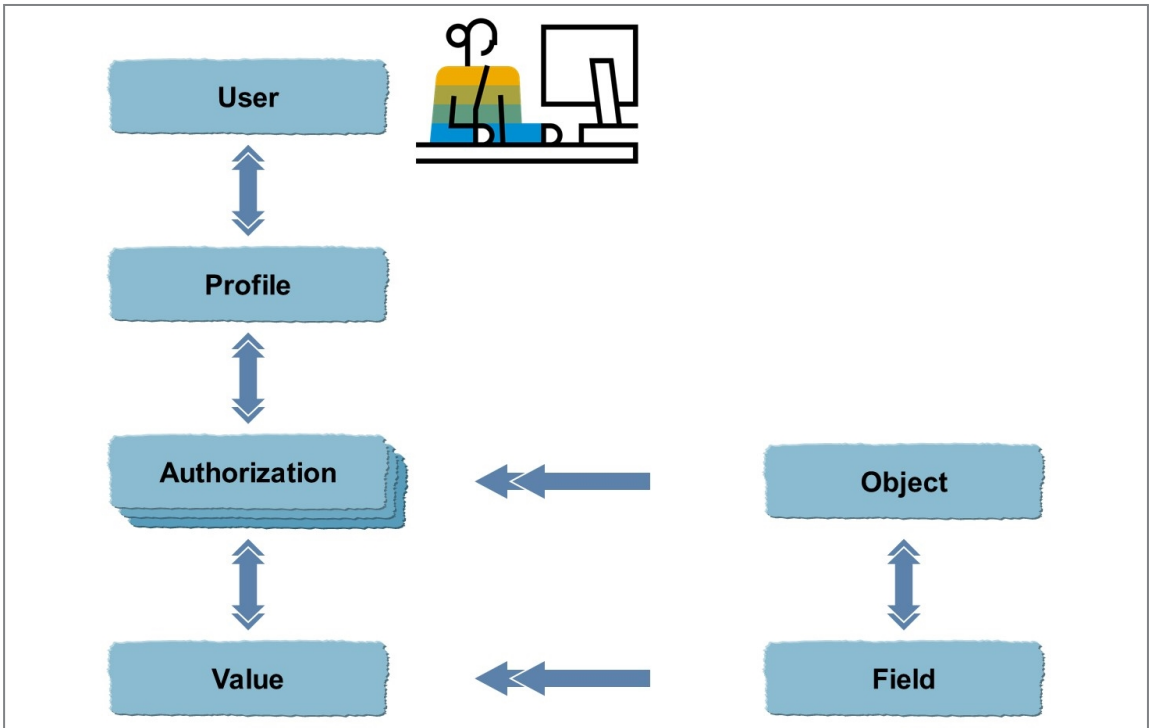

Figure 2: General Authorization Check

The general authorization check in SAP ERP HCM controls access to HR infotypes and forms a part of the general SAP authorization check.

You can define the following with authorization objects:

- Authorizations
- The fields that comprise an authorization, up to a maximum of 10 fields

When you define an authorization, the system checks the user master record to determine whether the specified user has the corresponding authorization to access the specified fields.

You define authorizations for an authorization object by specifying values for the individual fields of the object. You can create any number of authorizations, each with different values and names, for an authorization object.

Authorizations are grouped together in an authorization profile.

A user's authorizations are determined from the authorization profiles assigned to the user in the master data record for the various authorization objects in the system.

Structural Authorization Check

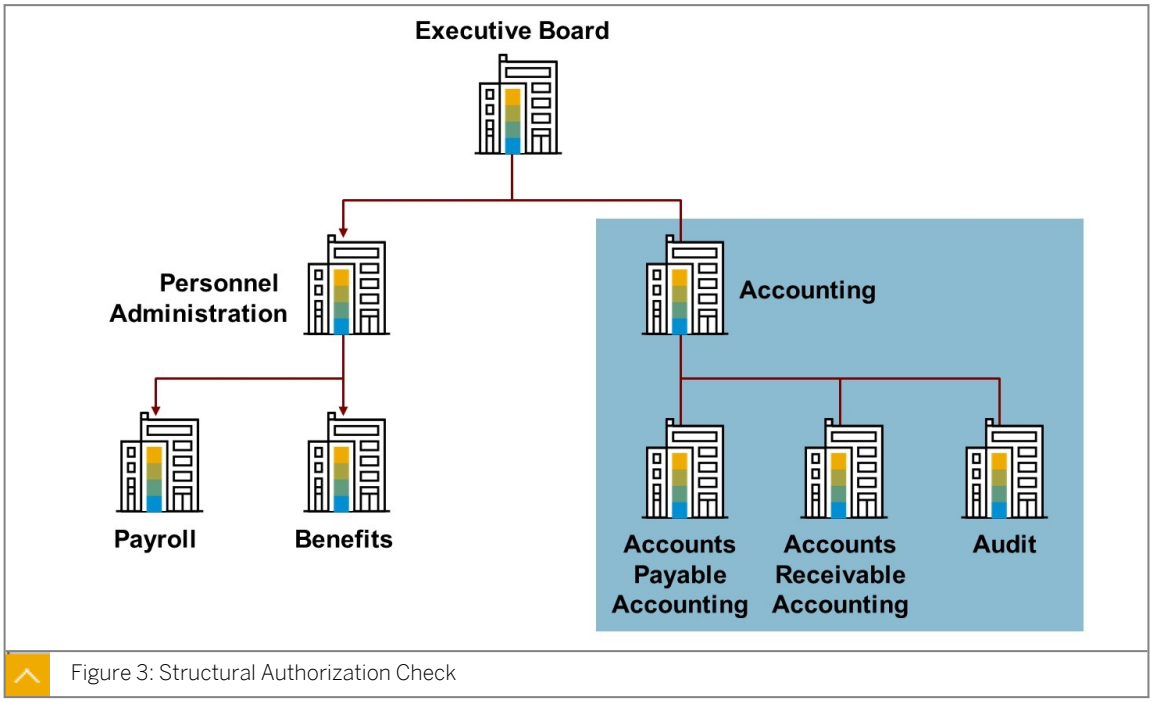

Figure 3: Structural Authorization Check

From a business point of view, the structural authorization check performs the same function as the general authorization check in SAP ERP HCM. Structural authorization controls access to data stored in time-dependent structures, such as organizational structures, course hierarchies, qualifications catalogs, and so on.

The flexibility of this concept ensures that the maintenance of structural authorizations is minimal, even if a change is made within the structure. This check ensures that users still have access only to those objects for which they are responsible.

LESSON SUMMARY

You should now be able to:

- Outline HCM authorization types
- Outline the general authorization check
- Outline the structural authorization check

Creating User Master Records

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Create a user master record for an existing employee

User Master Records

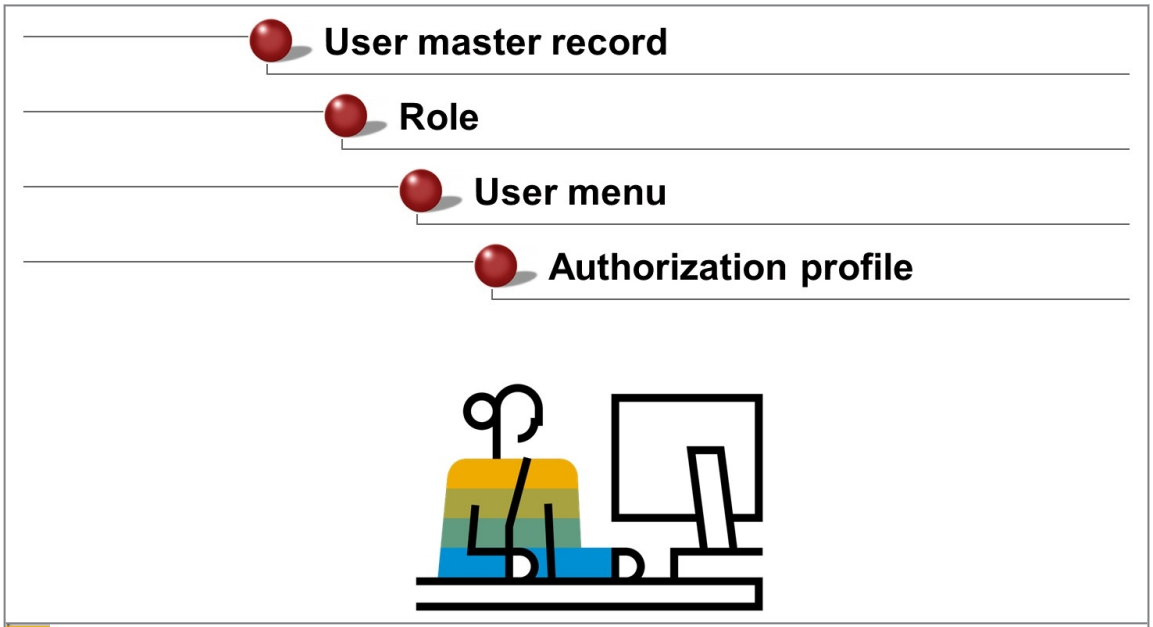

Figure 4: Users and Roles

To log on to the SAP system, a user must have a user master record and a corresponding password. In the user master record, a user menu and the corresponding authorization profiles are assigned to the user. This is done by assigning the user to one or several roles.

The following table defines the terms that are relevant to user master records:

Table 1: Terms and Descriptions

Term	Description
Role	A role is a collection of activities that enable a user to participate in one or more business scenarios in the organization. The assignment of users to roles safeguards the integrity of business data.

Term	Description
User menus	User menus provide access to the transactions, reports, or Web-based applications contained in the roles. A user menu should contain only the functions that a user typically performs at work.
Authorization profile	An authorization profile is generated for the activities contained in the role. This authorization profile defines the boundaries within which the user may perform actions in the SAP system.

LESSON SUMMARY

You should now be able to:

- Create a user master record for an existing employee

Copying SAP-Delivered Roles

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Copy sample roles delivered by SAP

HCM Role Profiles

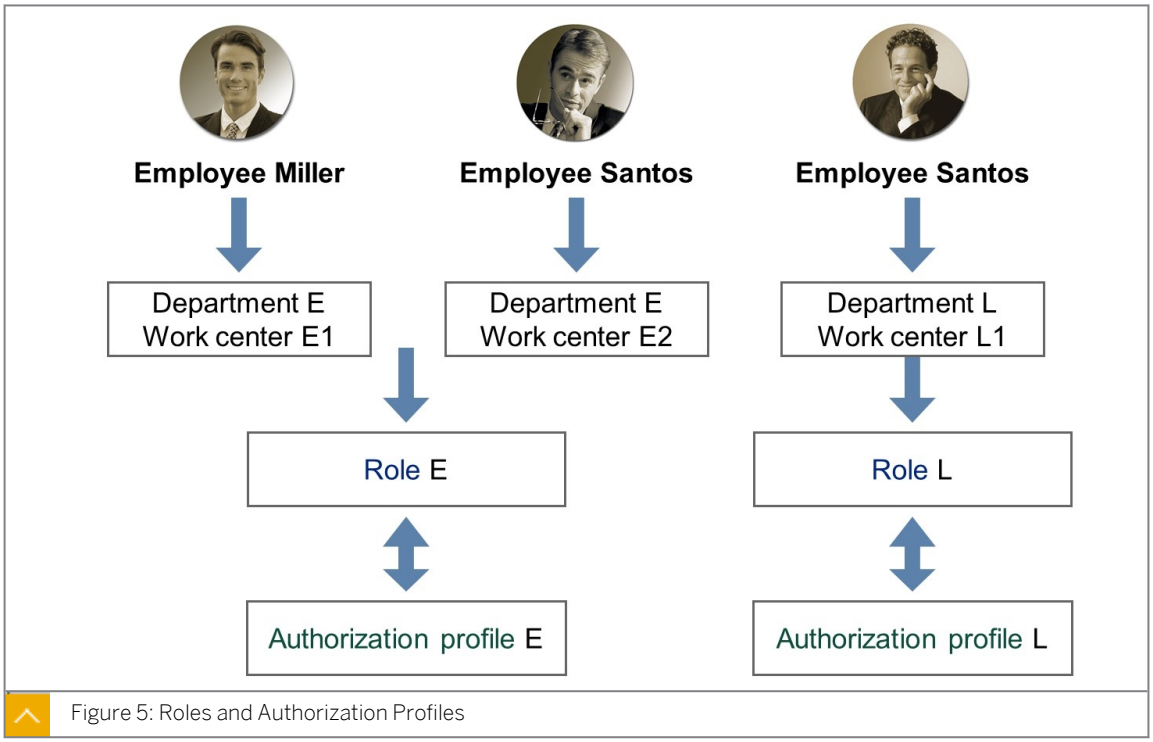

Figure 5: Roles and Authorization Profiles

The authorizations that an employee needs to access certain objects in the SAP system depend on the activities that an employee performs at work.

The authorizations required for a specific task area (role) in an enterprise are grouped together in an authorization profile.

To create or copy a role, execute the role maintenance transaction PFCG, search for and display the required role. Select transactions and menu paths. The selected functions correspond to the task area of a user or a group of users.

The profile generator provides the corresponding authorizations for the selected functions automatically. You can generate an authorization profile from these authorizations.

In the current release, SAP provides many single roles from all application areas. You will find the roles for human resources under the generic name SAP_HR*. You can copy these roles unchanged or you can copy them, change them, and then assign them to users.

Editing Roles - Example (1)

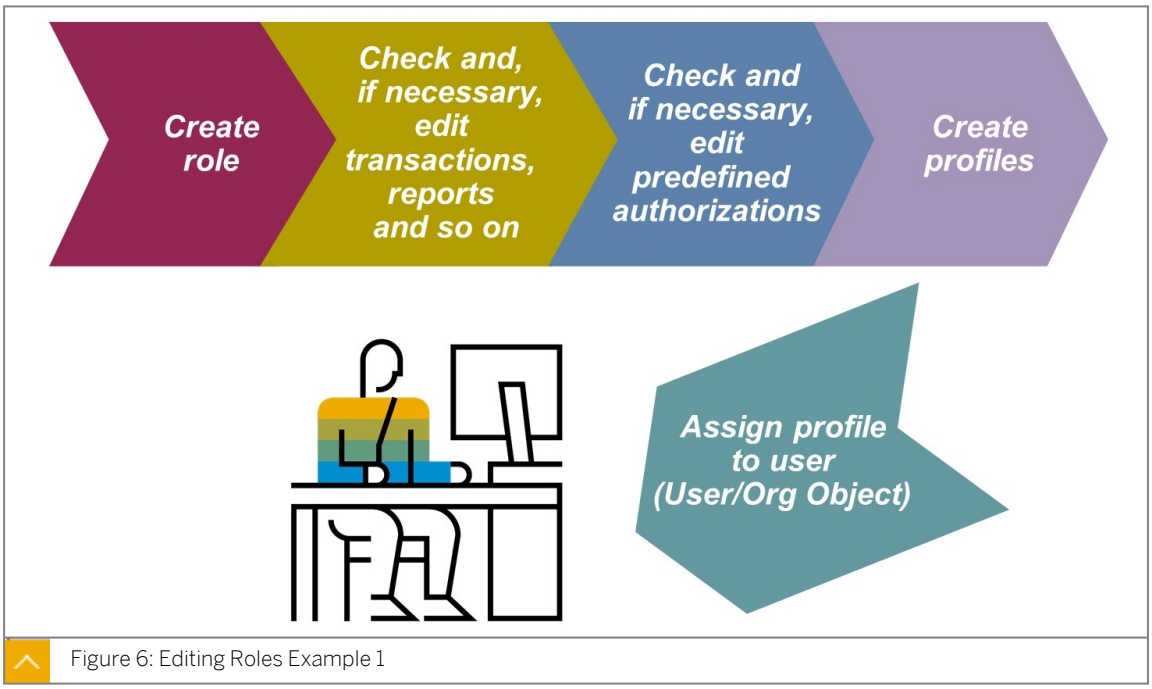

Figure 6: Editing Roles Example 1

You set up authorizations in the form of roles using the profile generator. Roles provide a business perspective by representing the tasks and activities that a user is authorized to perform in the system. Authorizations are parts of roles and are generated by the profile generator. You can generate several authorization profiles for each role.

When you generate roles, you also define the authorization objects with the necessary field specifications.

User menus provide access to the transactions, reports, or Web-based applications contained in the roles. A user menu should only contain the functions that are required by a specific user with a specific task profile for daily work.

To start the profile generator, on the *SAP Easy Access* screen, enter transaction `PFCG` in the *Command* field. To create a new role, choose the *Create Role* button.

The roles delivered by SAP begin with the prefix *SAP_*. To create your own user roles or copy existing ones, do not use the SAP namespace.

Editing Roles -Example (2)

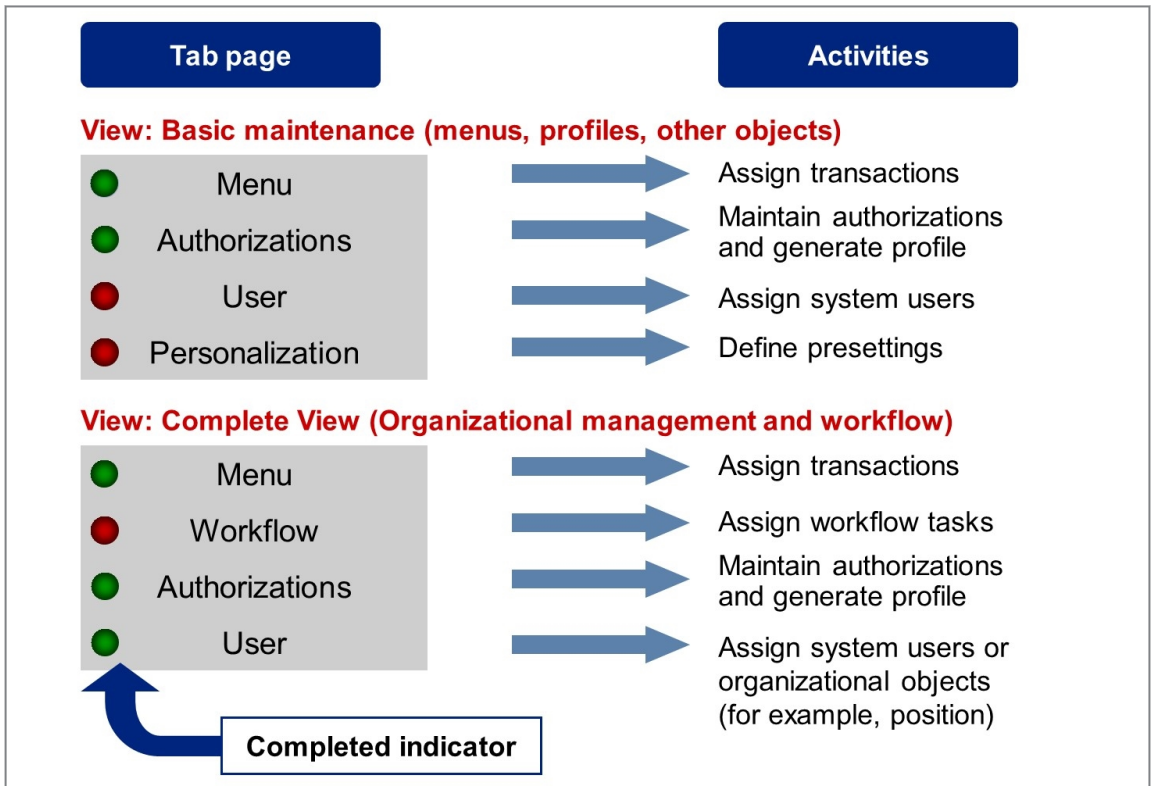

Figure 7: Editing Roles - Example (2)

On the *Menu* tab page, assign transactions, reports, or Web addresses to the role. By doing this, you set the user menu that is automatically displayed when the user assigned to this role logs on to the SAP system. When you assign transactions, the user's role or task profile is defined. The system then uses the transactions defined on the *Menu* tab page to create authorizations automatically.

If necessary, you can change the authorizations that the system automatically created when it generated the *Authorizations* tab page. To change authorizations, on this tab page, choose *Expert Mode* under *Maintain Authorization Data and Generate Profile*.

You can, for example, create additional authorizations when you change the authorizations that you have already created by choosing additional authorization objects.

After finishing required modifications to the automatically created authorizations, generate the authorization profile belonging to the role on the *Authorizations* tab page.

Finally, on the *User* tab page, assign users to the generated role. You can also assign users to roles through user master records or through organizational management objects (for example, job).

The generated profile is entered in the user master record only after a user comparison has occurred.

LESSON SUMMARY

You should now be able to:

- Copy sample roles delivered by SAP

Learning Assessment

1. General authorization and structural authorization can be used in combination.

   Determine whether this statement is true or false.

   ☐ True

   ☐ False

2. What are the prerequisites for using structural authorizations?

   _____

   _____

   _____

3. Structural authorization check can be used to control access to which of the following structures?

   Choose the correct answers.

   ☐ **A** Organizational structures

   ☐ **B** Human Resources infotypes

   ☐ **C** Qualifications catalogs

   ☐ **D** Course hierarchies

4. Why is it important to assign a user or an organizational object to a role?

   Choose the correct answers.

   ☐ **A** It safeguards the integrity of business data.

   ☐ **B** It defines the boundaries within which the user may perform actions in the SAP system.

   ☐ **C** It provides the user access to all the reports.

   ☐ **D** It helps define authorization profiles.

Learning Assessment - Answers

1. General authorization and structural authorization can be used in combination.

   Determine whether this statement is true or false.

   [X] True

   [ ] False

   Correct. General authorization and structural authorization can be used in combination.

2. What are the prerequisites for using structural authorizations?

   To use structural authorizations, ensure that your enterprise's structure is mapped in Organizational Management.

3. Structural authorization check can be used to control access to which of the following structures?

   Choose the correct answers.

   [X] A Organizational structures

   [ ] B Human Resources infotypes

   [X] C Qualifications catalogs

   [X] D Course hierarchies

   Correct. You can use structural authorization check to control access to organizational structures, qualification catalogs and course hierarchies.

4. Why is it important to assign a user or an organizational object to a role?

   Choose the correct answers.

   [X] A It safeguards the integrity of business data.

   [X] B It defines the boundaries within which the user may perform actions in the SAP system.

   [ ] C It provides the user access to all the reports.

   [ ] D It helps define authorization profiles.

   Correct. It is important to assign a user or an organizational object to a role, because it defines the boundaries within which the user may perform actions in the SAP system.

UNIT 2 General Authorization Checks

UNIT OBJECTIVES

- Outline HCM authorization objects
- Outline the process of checking master data storage on infotypes during authorization checks
- Outline the authorization check used when HR infotypes are edited or read
- Outline the personnel number check used to control user access to personal information

- Set up authorizations for an administrator
- Define SAP E-Recruiting authorization objects
- Define the Personnel Planning authorization objects
- Define authorizations for HR transactions without authorization objects
- Assign HR cluster data authorization to administrators
- Define customer-specific HR authorization objects
- Outline the asymmetrical double verification principle
- Outline the symmetrical double verification principle
- Set up a double verification for administrators

Outlining HCM Authorization Checks

LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Outline HCM authorization objects
- Outline the process of checking master data storage on infotypes during authorization checks
- Outline the authorization check used when HR infotypes are edited or read
- Outline the personnel number check used to control user access to personal information

HCM Authorization Objects

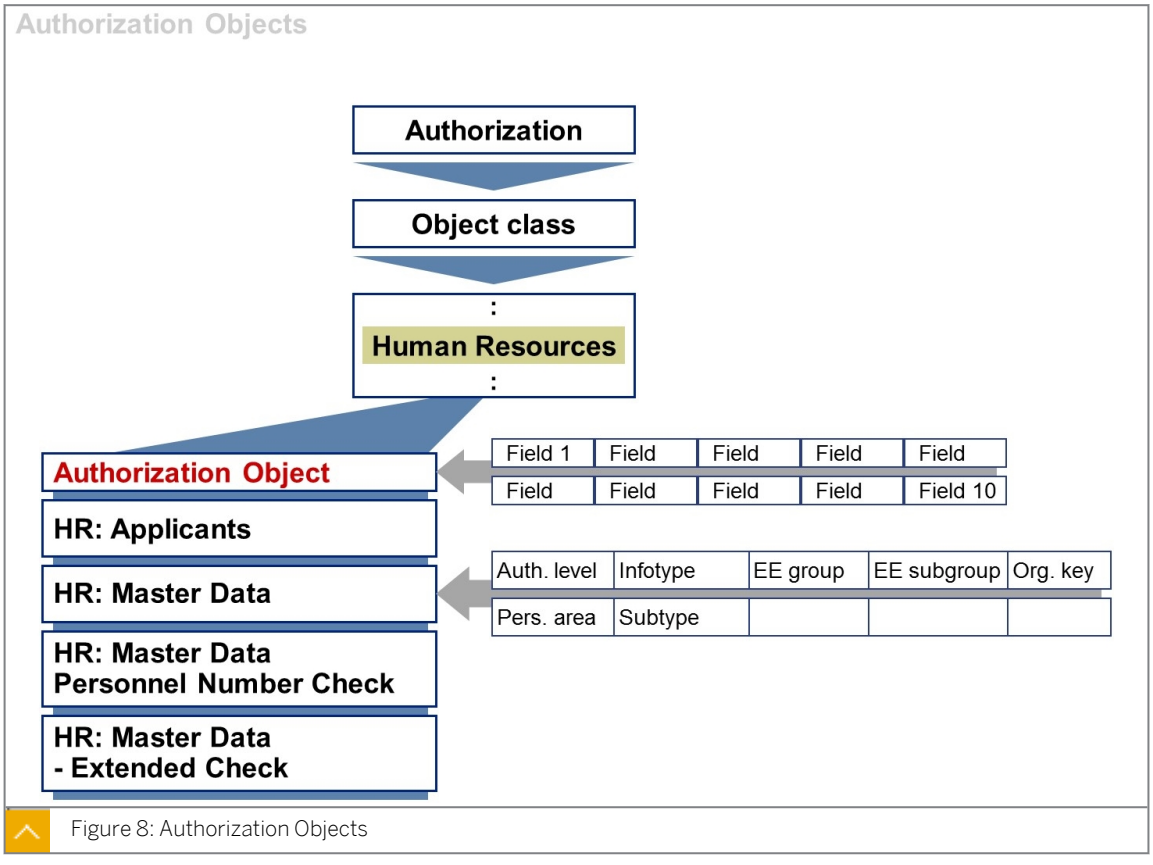

Figure 8: Authorization Objects

The figure Authorization Objects shows a number of authorization objects that you can use to define authorizations for SAP ERP HCM. Display these authorization objects using transaction `SU21` (HR object class) in the SAP system.

Authorization objects enable complex checks of an authorization, which allow a user to carry out an action. An authorization object groups up to 10 authorization fields that are checked in an AND relationship.

For a successful authorization, all field values of the authorization object must be maintained by the individual responsible for the configuration of authorizations. Authorization object fields are not considered input fields on a screen. Instead, they are system elements, such as infotypes, which must be protected.

> Note:
> In the SAP documentation, you can find information about maintaining authorization values.

You can define as many system access authorizations as you need for an object by creating several allowed values for the fields in the object. These value sets are called authorizations. The system checks these authorizations in OR relationships.

Master Data Authorizations

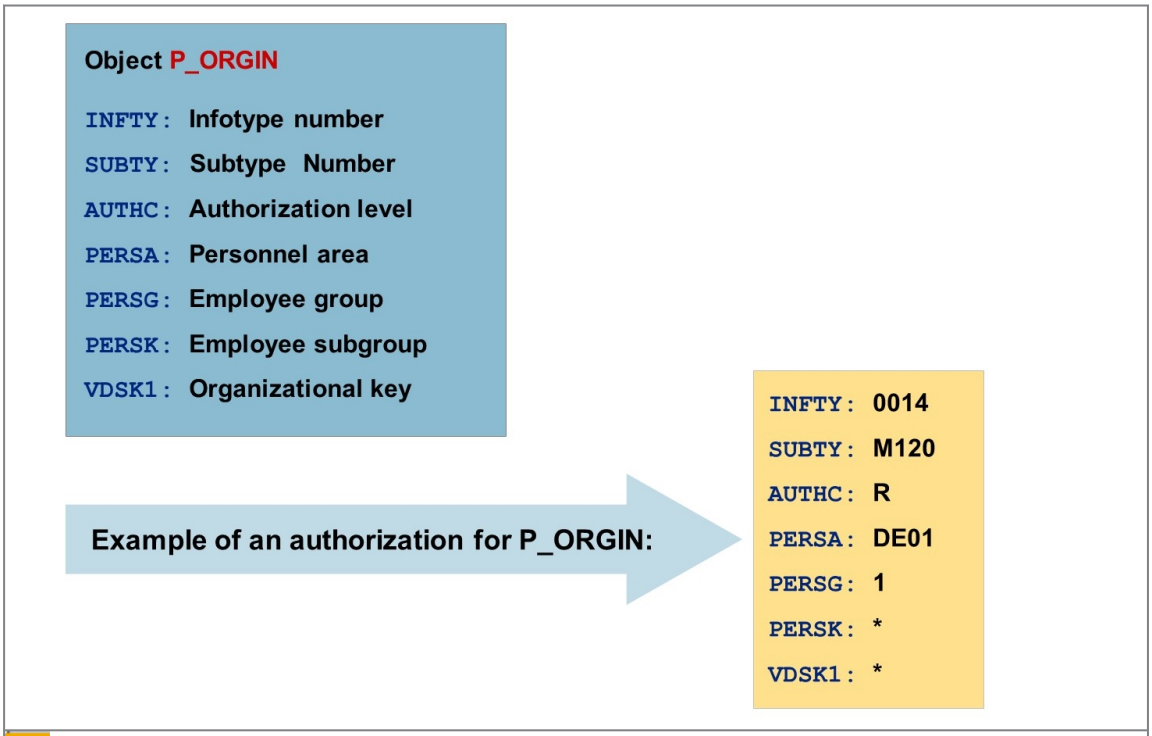

Figure 9: HR: Master Data

The *HR: Master Data* authorization object is used during the authorization check on HR infotypes. The authorization check takes place when HR infotypes are edited or read. The system queries the contents of the fields during the check.

Authorization Levels

The Authorization level field specifies the access mode. The following authorization levels exist:

Table 2: Authorization Levels

Authorization Level	Description	Access Mode
R	Read	Read access
M	Matchcode	Read access using input help (F4)
W	Write	Write access
E and D	Enqueue and Dequeue	Write access using the asymmetrical double-verification principle; E allows the user to create and change locked data records, D allows the user to change lock indicators
S	Symmetrical	Write access using the symmetrical double-verification principle
*	All authorization levels	Always includes all other authorization levels simultaneously

Extended Check Authorization

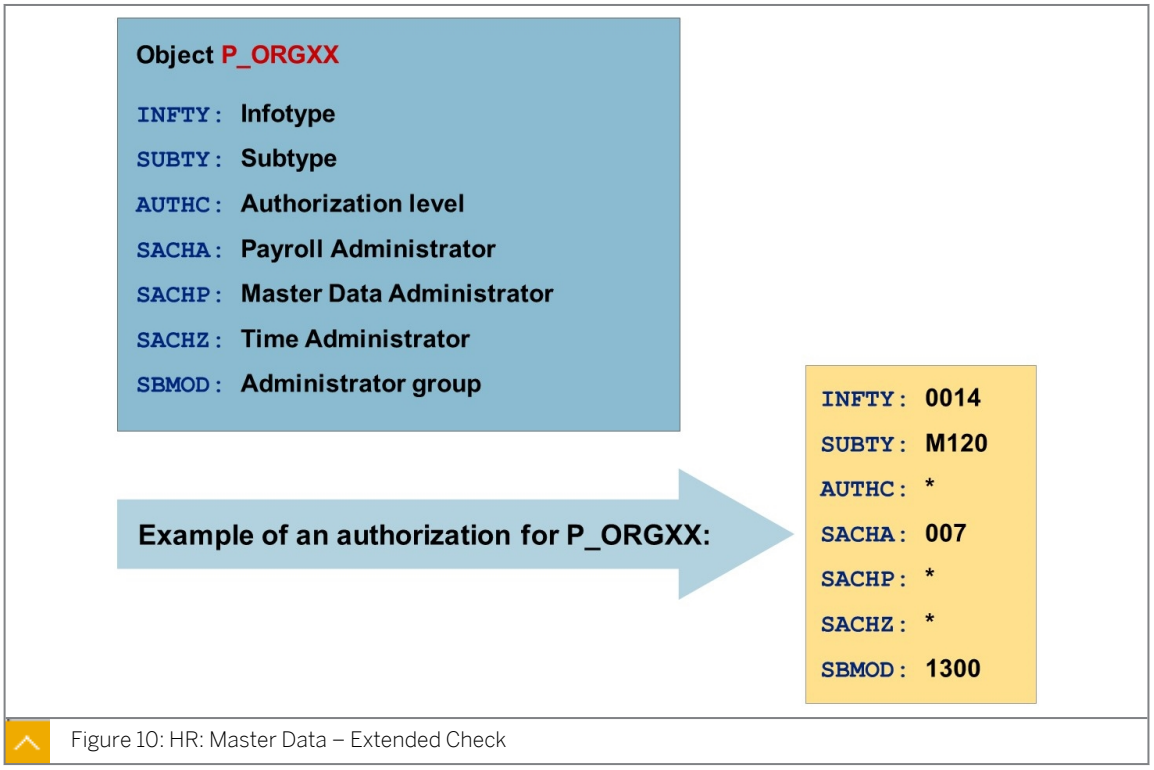

Figure 10: HR: Master Data – Extended Check

The system uses the object *HR: Master Data – Extended Check* during the authorization check on HR infotypes. The checks take place when HR infotypes are edited or read.

The fields *SACHA*, *SACHP*, *SACHZ*, and *SBMOD* are filled from the *Organizational Assignment* infotype (0001). This infotype has time-dependent specifications and an authorization may exist only for certain time intervals, depending on the user's authorization. A user's period of responsibility is represented by all the time intervals for which the user has P_ORGXX authorizations.

All administrators responsible for an organizational area in Personnel Administration are grouped together in the administrator group.

In an SAP standard system, this extended check is not active. You can use the main authorization switch (transaction `OOAC`) to determine whether this check is to be carried out in addition to or instead of the *HR: Master Data Check*.

If the additional check is activated, the system performs an authorization check according to *HR: Master Data*. If the check result is positive, the system performs a further check according to *HR: Master Data – Extended Check*.

Personnel Number Check

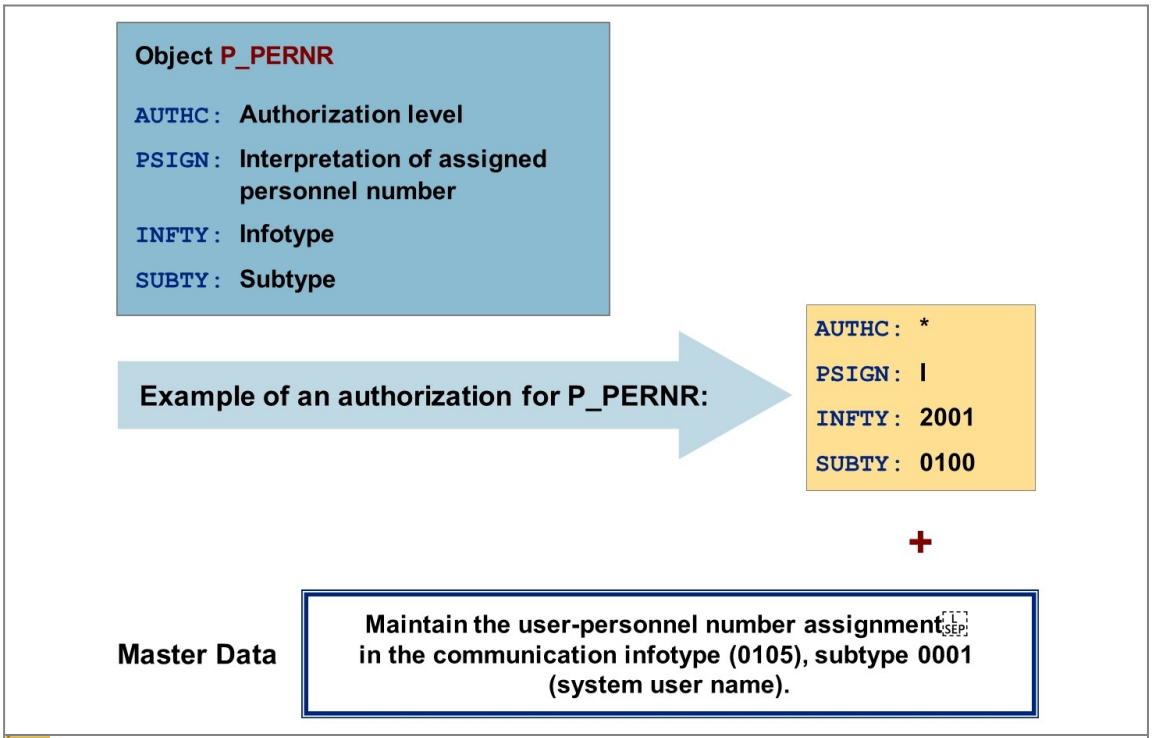

Figure 11: HR: Master Data – Personnel Number Check

The authorization object *HR: Master Data – Personnel Number Check* is used when you want to assign users different authorizations for accessing their own personnel number. If this check is active and the user is assigned a personnel number in the system, this check directly overrides all other checks except for test procedures.

The following values are possible for the PSIGN field:

- I = Authorization for the user's own personnel number is included.
- E = Authorization for the user's own personnel number is excluded.

You can assign a user a personnel number using infotype 0105, subtype 0001.

The *HR: Master Data - Personnel Number Check* does not take place for a user that is not assigned to a personnel number, or if the user accesses a personnel number other than his or her own. This check is irrelevant for personnel numbers that are not assigned to a user.

Personnel Number Check – Example 1

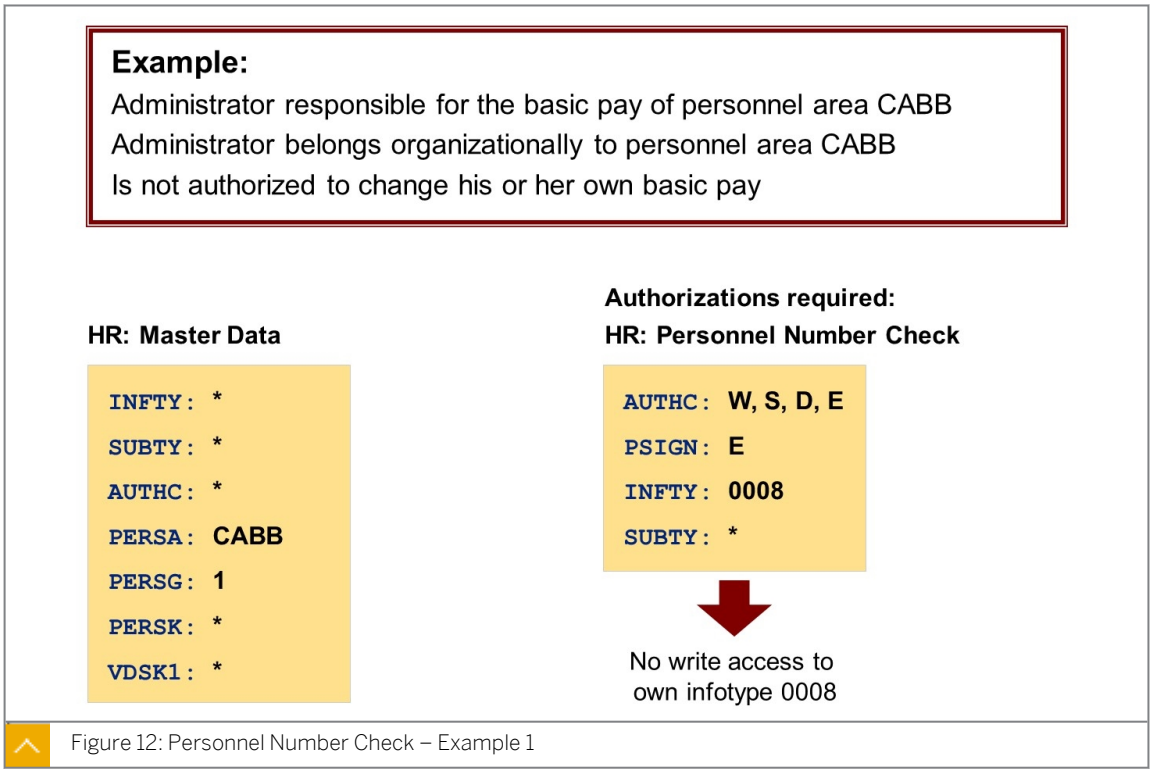

Figure 12: Personnel Number Check – Example 1

The figure Personnel Number Check - Example 1 illustrates an example of a user who is an administrator, responsible for the *basic pay* (infotype 0008) of a personnel area. The user has the corresponding *HR: Master Data authorization* for personnel area CABB. The user must be able to display personal data at all times but not be able to change his or her own basic pay, regardless of the personnel area of responsibility.

The authorization for the object *HR: Personnel Number Check* must be set as indicated in this example.

This authorization enables the following infotype access:

- The first authorization grants the user read authorization for all infotypes stored under the user's personnel number.
- The second authorization denies write authorization for all data records of infotype 0008 stored under the user's personnel number.

Hint:
If you use personnel number-based authorizations, you must first set up all the authorizations that are not based on personnel numbers. Then, you must create different access authorizations for the personnel numbers assigned to users using appropriate P_PERNR authorizations. The P_PERNR authorizations override all other authorizations directly (except test procedures).

Personnel Number Check – Example 2

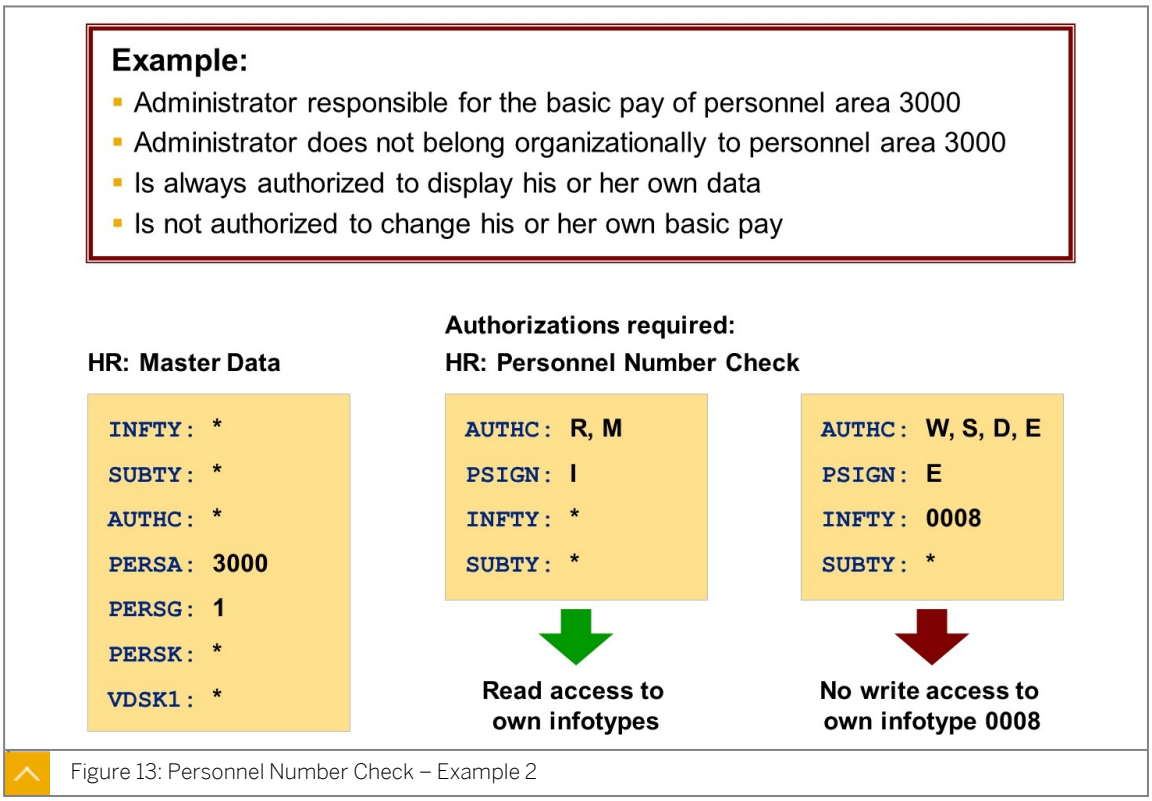

Figure 13: Personnel Number Check – Example 2

In this example, the user is an administrator responsible for the basic pay (infotype 0008) of a personnel area. The user has the corresponding *HR: Master Data* authorization for personnel area 3000. The user must be able to display personal data at all times but not be able to change his or her own basic pay, regardless of the personnel area of responsibility.

The authorization for the object *HR: Personnel Number Check* must be set as in this example.

This authorization enables the following infotype access:

- The first authorization grants the user read authorization for all infotypes stored under the user's personnel number.
- The second authorization denies write access to all data records of infotype 0008 for the user's own personnel number if the user becomes responsible later for the personnel area to which he or she belongs.

Flowchart: Personnel Number Check

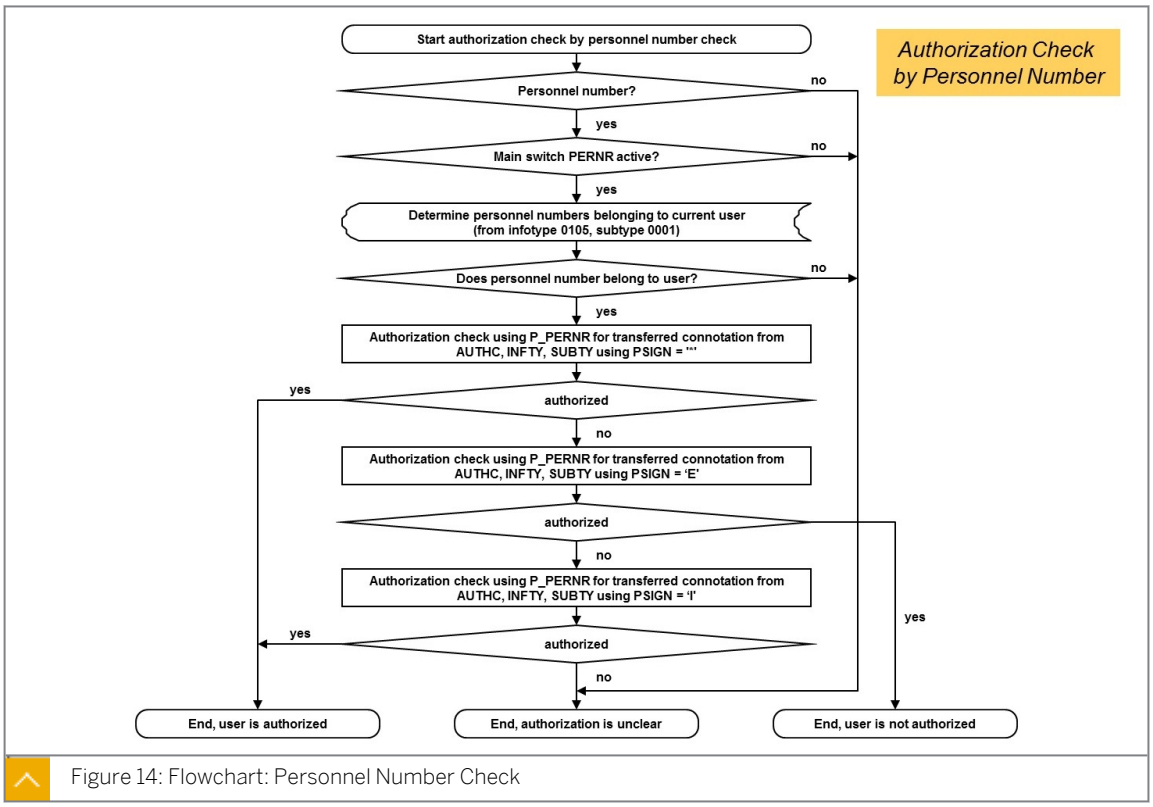

Figure 14: Flowchart: Personnel Number Check

The figure illustrates a typical flowchart for a personnel number check.

LESSON SUMMARY

You should now be able to:

- Outline HCM authorization objects
- Outline the process of checking master data storage on infotypes during authorization checks
- Outline the authorization check used when HR infotypes are edited or read
- Outline the personnel number check used to control user access to personal information

Setting Up an Authorization

LESSON OVERVIEW
This lesson describes the set up of authorization switches.

Business Example

You need to set up new authorizations for Human Resources administrators while ensuring appropriate restrictions so that they are allowed to change only certain aspects of their own data. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Set up authorizations for an administrator

Authorization Main Switches

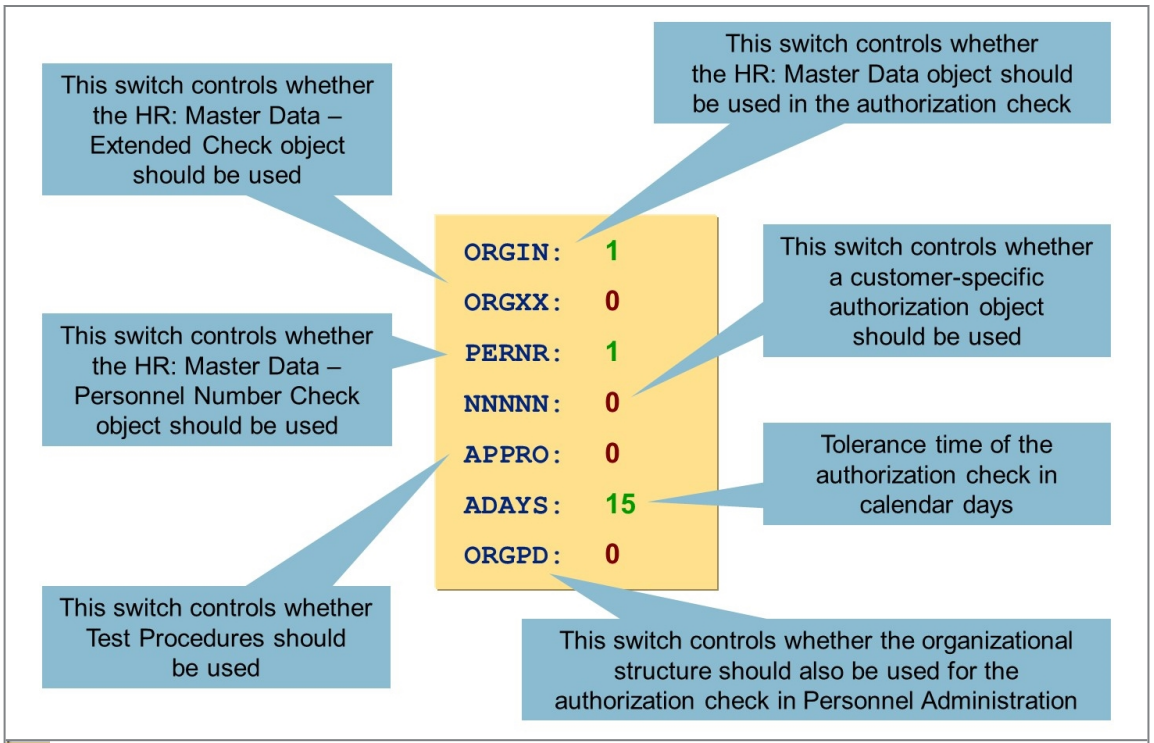

Figure 15: Authorization Main Switches

The authorization main switches are stored in Table T77S0 under the group name AUTSW.

You can use these switches to adjust the behavior of the authorization check on HR infotypes to meet your requirements. You can also specify the switch settings at the client level differently.

The figure Authorization Main Switches illustrates the standard switch settings.

You can use the master data check (ORGIN) and the extended check (ORGXX) together, in which case - both switches are set to 1 - or alternatively, in which case only one of the switches is set to 1.

Hint:
You can configure the settings using transaction OOAC or in Customizing for Personnel Administration. Choose *Tools → Authorization Management → Edit Authorization Main Switch*.

LESSON SUMMARY
You should now be able to:

- Set up authorizations for an administrator

Defining SAP E-Recruiting Authorization Objects

LESSON OVERVIEW
This lesson describes the authorization objects used in SAP E-Recruiting.

Business Example

Your company uses SAP E-Recruiting and as a member of the project team, you are responsible for the set up authorization objects. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Define SAP E-Recruiting authorization objects

Roles in SAP E-Recruiting

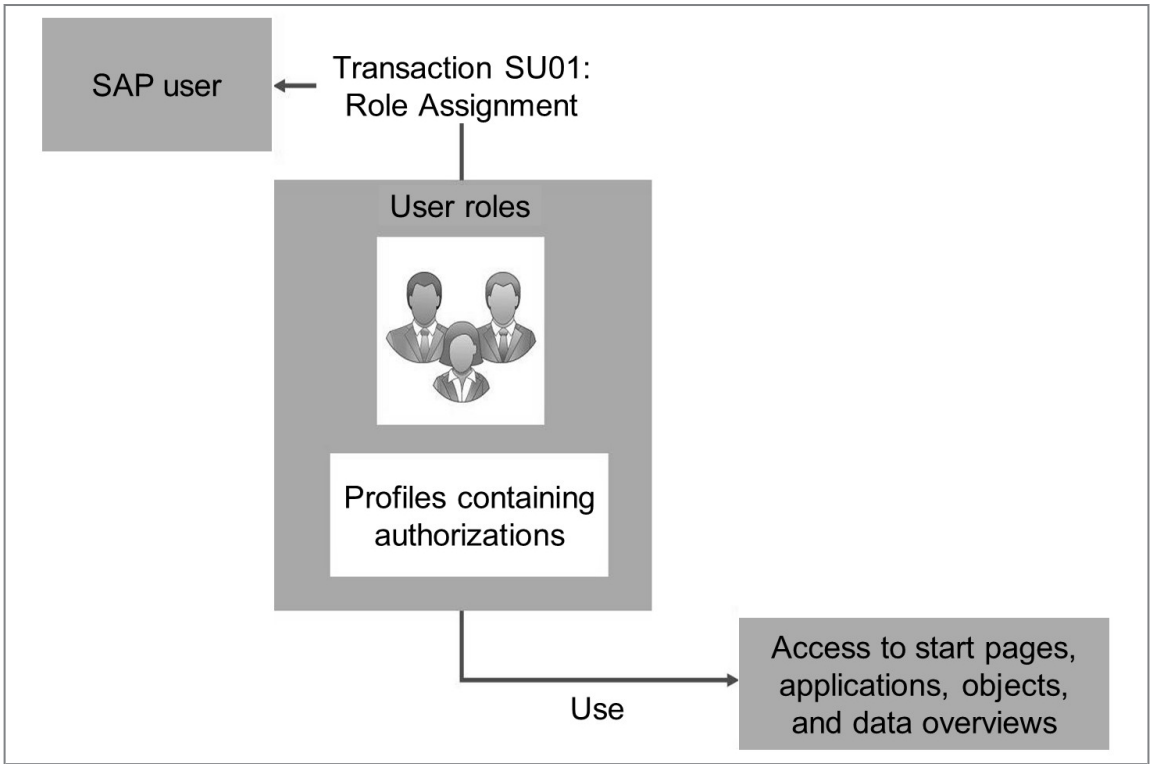

Figure 16: Roles in SAP E-Recruiting

SAP provides a range of authorization roles for E-Recruiting. These correspond to the preconfigured roles of E-Recruiting that control the user interface and working interface.

Portal Agnostic (Portal-Free) Roles

HCM, including SAP E-Recruiting and roles (for example, the HR administrator and Employee Self–Service [ESS]), is available through the portal as well as through SAP NetWeaver Business Client (NWBC). Activation of Business Function HCM_NWBC_ROLES is necessary.

The following NWBC roles are available:

- Recruiter
- Recruiting Administrator

The following roles can be run without a portal by using SAP NetWeaver Business Client for HTML:

- Manager (MSS)
- HR Administrator
- Employee (ESS)

Portal Agnostics – Roles and Authorizations

The authorization roles for menu navigation are as follows:

- SAP_RCF_ESS_SR_ERC_CI_4: E-Recruiting services for ESS.
- SAP_RCF_MSS_SR_ERC_CI_4: E-Recruiting services for MSS.
- SAP_RCF_RECRUITER_SR_ERC_CI_4: Recruiter NWBC.
- SAP_RCF_REC_ADMIN_SR_ERC_CI_4: Recruiting Administrator NWBC.
- SAP_ASR_HRADMIN_SR_HCM_CI_3: HR Administrator (New Hire scenario).

There are new roles available as of EhP5 (transaction `PFCG`) that can be used as copy templates for customer roles. These roles contain all necessary authorizations needed to use the corresponding Web Dynpro applications without using the SAP portal. The roles drive the menus (navigation) for each user in NWBC for HTML environment. In addition to these roles, the known SAP E-Recruiting roles must be assigned to the profiles of the relevant users to ensure that all services can be executed.

The new PFCG roles are used to define the UI structure when using the HTML (ABAP) version of NWBC. There is one dedicated 'single role' (with '_SR_') in its name, which only defines the role menu (UI).

This role is combined with one of the following standard authorization roles to form a composite role:

- Recruiter

  SAP_RCF_RECRUITER_SR_ERC_CI_4 used in composite role SAP_RCF_RECRUITER_ERC_CI_4.

- Recruiting Administrator

  SAP_RCF_REC_ADMIN_SR_ERC_CI_4 used in composite role SAP_RCF_REC_ADMIN_ERC_CI_4.

- Candidate

  SAP_RCF_ESS_SR_ERC_CI_4 used in composite role SAP_EMPLOYEE_ESS_WDA_1.

- Manager

  SAP_RCF_MSS_SR_ERC_CI_4 used in composite role SAP_MANAGER_MSS_NWBC.

User Roles – Examples

The following table shows examples of user roles and their description:

Table 3: User Roles

User Role	Description of the Role
SAP_RCF_CONTENT_SERVER	Access to the Search and Classification (TREX) search engine
SAP_RCF_BUSINESS_ADMINISTRATOR	Administrator
SAP_RCF_DATA_TYPIST	Data entry clerk (authorization for minimum entry of applicant data)
SAP_RCF_DECISION_MAKER	Decision maker (for example, a manager who is forwarded a shortlist to decide which applicant is of interest)
SAP_RCF_EXTERNAL_CANDIDATE	External candidate (who can display and change individual data)
SAP_RCF_INTERNAL_CANDIDATE	Internal candidate (who can display and change individual data)
SAP_RCF_RECRUITER	Recruiter
SAP_RCF_RESTRICTED_RECRUITER	Restricted recruiter
SAP_RCF_UNREGISTERED_CANDIDATE	Unregistered candidate (for example, service users and public users)
SAP_RCF_MANAGER	Manager (this role enables access to the portal for Manager Self-Service [MSS])

The roles listed in the table are delivered in the standard system and can be implemented directly.

You can use these roles as copy templates when creating your own user roles. You need to create your own user roles, for example, if the authorization profiles have to be adjusted. You can create your own roles or assign a reference user to a role in *Customizing*.

To create your own roles or assign a reference user to a role in Customizing, choose *SAP E-Recruiting → Technical Settings → User Administration → Roles in E-Recruiting → Define Roles in E-Recruiting.*

The roles that can be changed, but must not be deleted are as follows:

- Candidate (internal)
- Manager
- Candidate (external)
- Recruiter
- Data entry clerk

- Requisition requester
- Decision maker

Authorization Objects

Authorization checks are performed when a user performs the following operations:

- Accessing a start page
- Logging on
- Accessing an application

Most authorizations in SAP E-Recruiting are assigned using authorization objects. However, there are some context-specific restrictions.

Examples of context-specific restrictions:

- Candidates can display and change only their own profiles. This authorization is not checked using authorization objects but rather within the relevant application (in the context of each application).
- A recruiter can view or change all candidate data.

An authorization object can have up to ten authorization fields that are checked using an AND operation.

Important Authorization Objects

Some examples of important authorization objects and the information they provide are shown in the following table:

Table 4: Authorization Objects

Authorization Objects	Description
P_RCF_APPL	Access applications
PLOG	Objects and infotypes (PLVAR 01 only)
P_TCODE	Required authorization check for qualifications → PP*
B_BUPA*	Basic authorizations for business partners (personal data managed in the business partner area)
P_RCF_POOL	Direct access to talent pool
P_RCF_STATUS	Object status in E-Recruiting
P_RCF_VIEW	Display data overviews
S_USER_GRP	Create candidates

You need to consider the following points about authorization objects:

- You can display the documentation for an authorization object by double-clicking the object. The documentation explains how to maintain the values for the object.
- You can display and maintain authorization objects through the profiles (transaction `PFCG`). The namespace for specific authorization objects in SAP E-Recruiting is P_RCF_*.

Authorization Object for Activities in SAP E-Recruiting

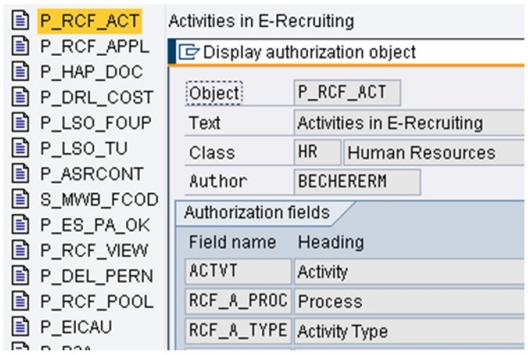

Figure 17: Authorization Object for Activities in SAP E-Recruiting

The authorization object P_RCF_ACT controls which users can edit which activities in SAP E-Recruiting.

The authorization object P_RCF_ACT contains the following authorization fields:

ACTVT (activity):

Controls how activities are created, changed and deleted.

RCF_A_PROC (process):

Specifies the process for which the authorization check is to be carried out.

RCF_A_TYP (activity type):

Specifies the activity type for which the authorization check is to be carried out.

You can also use the authorization object P_RCF_ACT to regulate the activities available to the user in the dialog box menu for creating activities.

You can maintain authorization objects using transaction `SU03` or `SU21`.

Example of the Authorization Object P_RCF_STATUS (1)

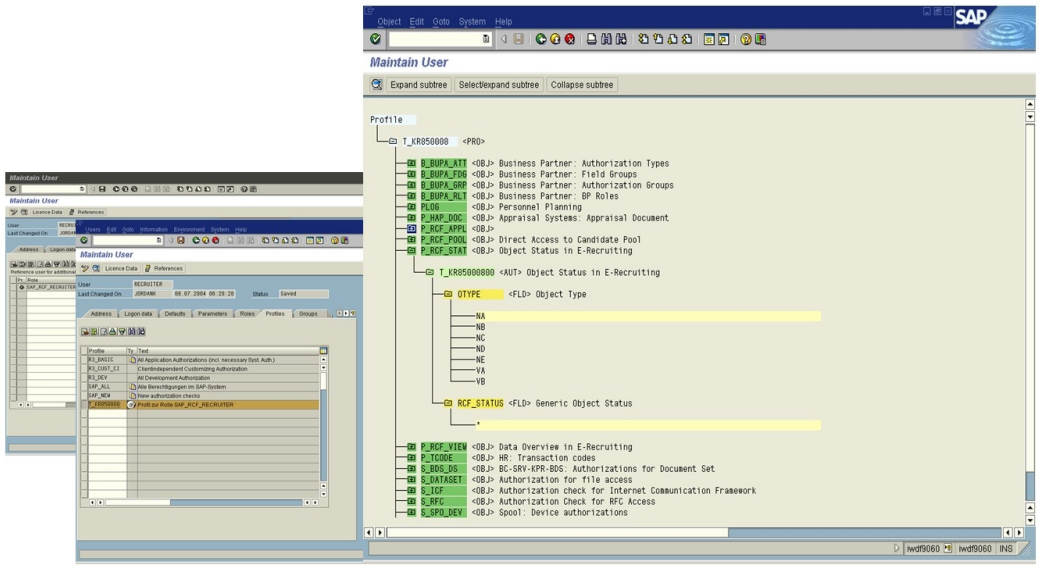

Figure 18: Example of the Authorization Object P_RCF_STATUS (1)

Authorization objects are grouped together in authorization classes. P_RCF_STATUS is an authorization object that is checked in SAP E-Recruiting each time there is a status change for the candidate, application, application selection, posting, requisition, or questionnaire.

The object type field defines the object types for which the user is permitted to make a status change.

Example of the Authorization Object P_RCF_STATUS (2)

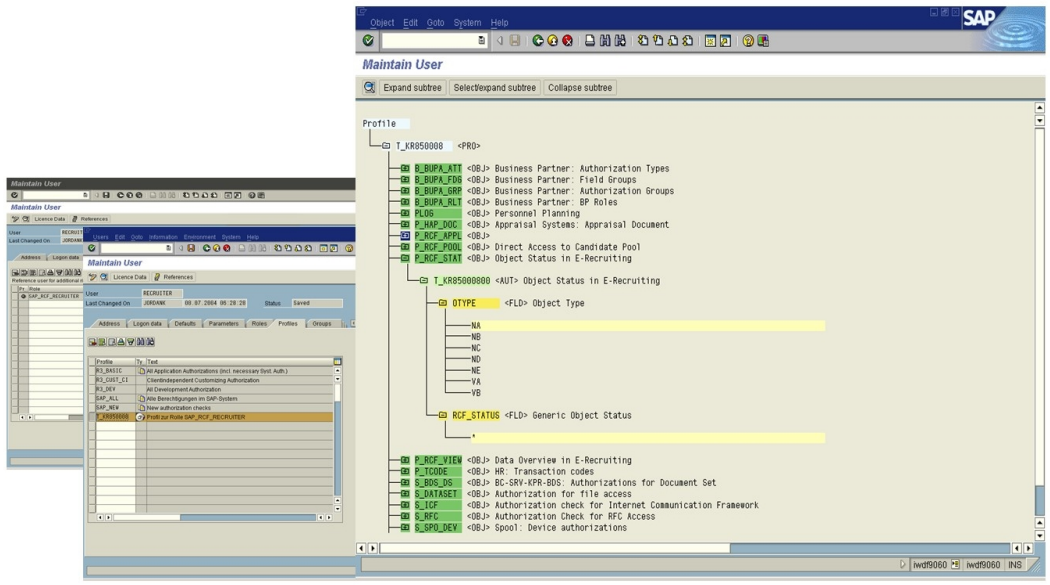

Figure 19: Example of the Authorization Object P_RCF_STATUS (2)

The *Generic Object Status* field determines the status that the user is permitted to set for a given object type.

Object Types

The following table shows the statuses that are checked for each object type:

Table 5: Status, checked for each object type

Object Type	Status
Candidate (NA)	• 0 – Locked • 1 – Released
Application (ND)	• 0 – Draft • 1 – In Process • 2 – Withdrawn • 3 – Rejected • 4 – To be hired

Object Type	Status
Candidacy (NE)	• 0 – In Process • 1 – Withdrawn • 2 – Rejected • 3 – To be hired • 4 – Draft
Requisition (NB)	• 0 – Draft • 1 – Released • 2 – Closed • 3 – To be deleted • 4 – On hold
Posting (NC)	• 0 – Draft • 1 – Released • 2 – Closed • 3 – To be deleted
Questionnaire (VA)	• 0 – Draft • 1 – Released • 2 – To be deleted
Question (VB)	• 0 – Draft • 1 – Released • 2 – To be deleted

Example of the Authorization Object P_RCF_APPL

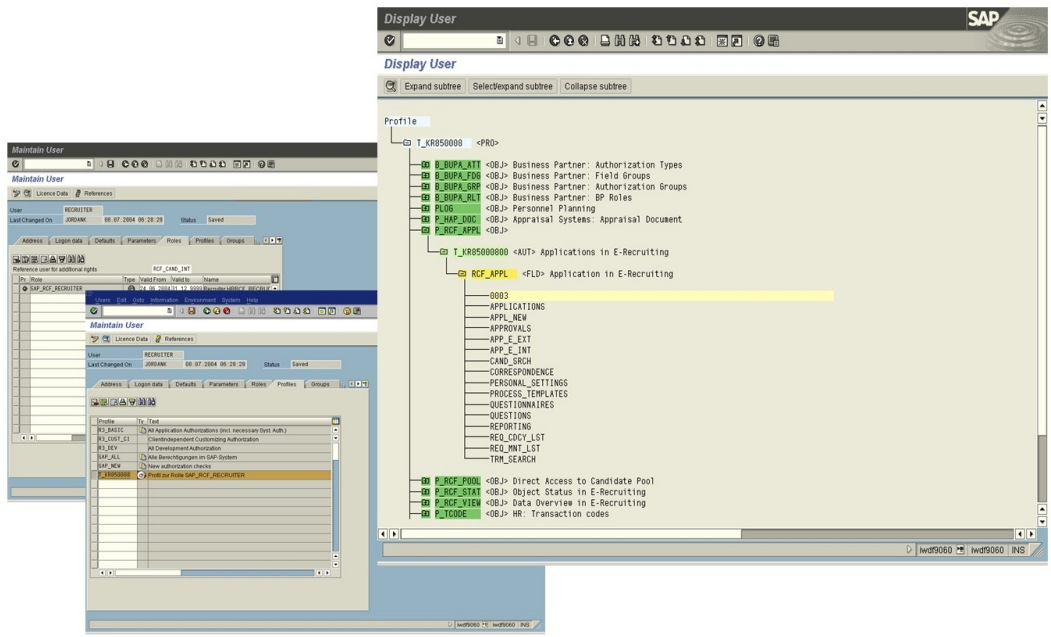

Figure 20: Example of the Authorization Object P_RCF_APPL

P_RCF_APPL is an authorization check that is run when calling the SAP E-Recruiting applications. The logical name of the application or the ID of the start page is checked in the *Application* field.

Users in SAP E-Recruiting

The following table displays the user types that exist in SAP E-Recruiting:

Table 6: Types of Users

User Type	Description
Dialog user	• For the various actors in SAP E-Recruiting such as external and internal candidates, and recruiters
Service user	• For anonymous or unregistered users, such as external persons who are not yet registered in the talent pool and are looking for a job • For Search and Classification (TREX) access • For public users (for example, users outside of the company)
Reference user	• Corresponds to a possible role in SAP E- Recruiting; each role requires a reference user to start the application that corresponds to the role of the reference user before the actual user can log on to the system

User Type	Description
System user	• For background processing, such as Work Flow (WF) batch (authorization required to create requisitions and to change the status) and e-mail address required for correspondence

LESSON SUMMARY

You should now be able to:

- Define SAP E-Recruiting authorization objects

Defining Personnel Planning Authorization Objects

LESSON OVERVIEW
This lesson outlines personnel planning authorization objects.

Business Example:

As a member of the authorizations team, you are responsible for the set up of personnel planning authorizations. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Define the Personnel Planning authorization objects

Personnel Planning Authorization Objects

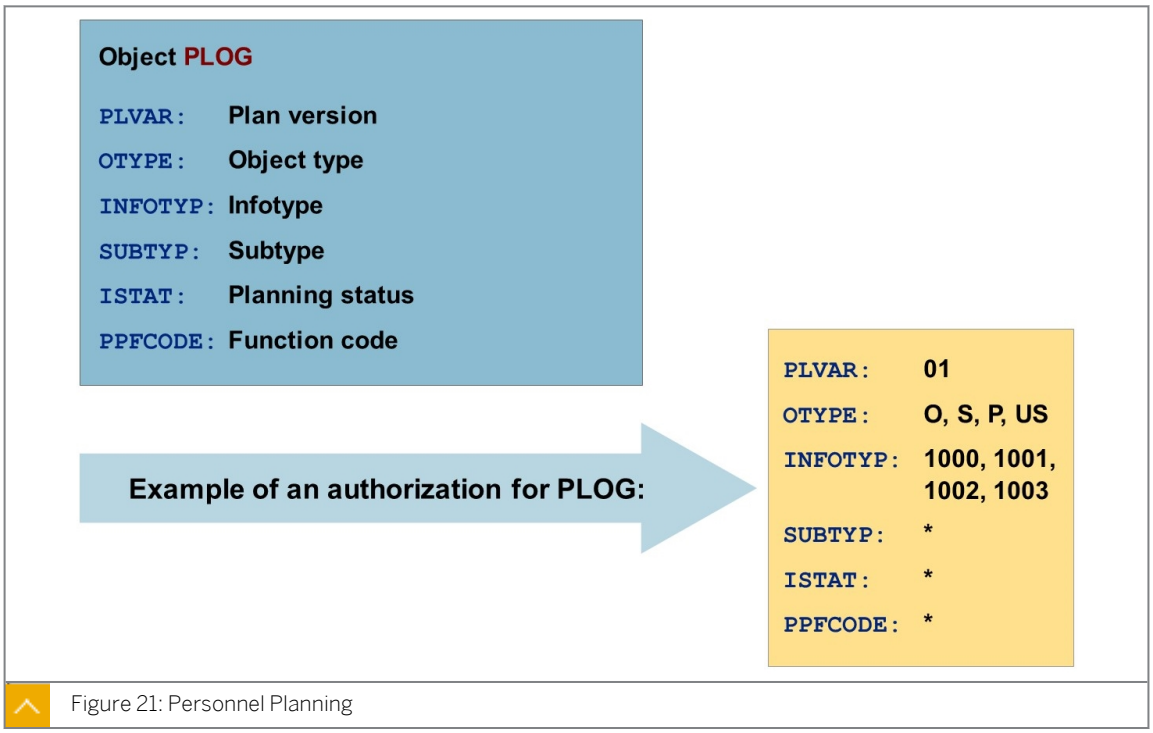

Figure 21: Personnel Planning

You can use authorization object PLOG to check the authorization for specific fields in the Personnel Planning components (such as Organizational Management, Personnel Development, Training and Event Management).

Plan version

This field specifies which plan versions the user is authorized to access.

Object type

This field specifies which object types the user is authorized to access.

Infotype

This field specifies which infotypes the user is authorized to access.

Subtype

This field specifies which subtypes of the infotypes the user is authorized to access.

Planning Status

This field specifies the planning status in which the user is authorized to access information.

Function Code

This field specifies the editing mode for which the user has authorization (display, change, and so on).

LESSON SUMMARY

You should now be able to:

- Define the Personnel Planning authorization objects

Unit 2
Lesson 5

Defining Transaction Code Authorizations

LESSON OVERVIEW

This lesson describes how the *HR: Transaction Code* object can be used to define Human Resources (HR) authorizations for the HR transactions that do not have their own authorization object.

Business Example

You need to set up authorizations for various HR transactions that do not have their own authorization object. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Define authorizations for HR transactions without authorization objects

Authorization Object HR: Transaction Code

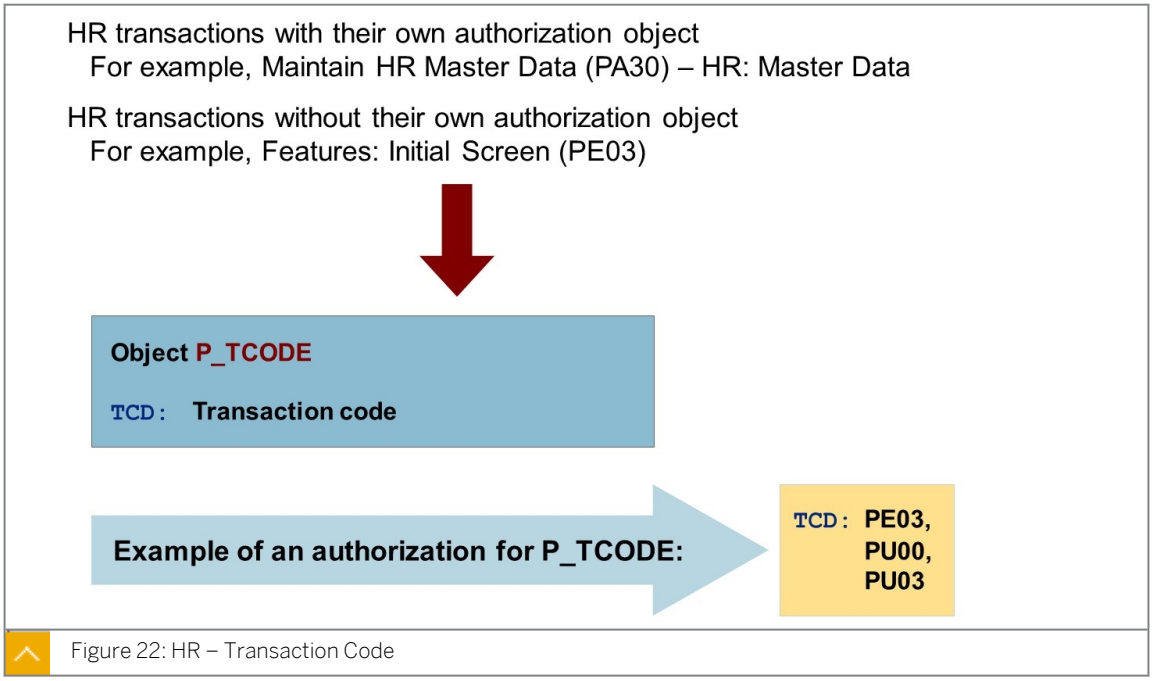

Figure 22: HR – Transaction Code

Authorization object P_TCODE, enables the system to check whether a user is authorized to start the different HR transactions. This authorization object checks the transaction code.

Note:
The object P_TCODE is not used in all HR transactions.

The HR transactions can be distinguished as follows:

- HR transactions with a natural (their own) authorization object.
- HR transactions without a natural (their own) authorization object.

The authorization object P_TCODE contains the HR transaction codes without their own authorization object.

P_TCODE is the HR equivalent of the Check Transaction Code at Start of Transaction authorization object (S_TCODE). The P_TCODE authorization object was implemented before the S_TCODE authorization object. Given the increased need to protect data in HR, P_TCODE was retained as a protective measure.

Hint:
Avoid modifying the authorization objects, S_TCODE and P_TCODE, directly. Instead, add additional transactions to your role's menu. The system, then, automatically enters these transactions in both authorization objects.

LESSON SUMMARY
You should now be able to:

- Define authorizations for HR transactions without authorization objects

Unit 2
Lesson 6

Assigning HR Cluster Data Authorizations

LESSON OVERVIEW
This lesson outlines HR Cluster Data Authorizations and how this authorization object is used.

Business Example:

As a member of the authorizations team, one of your responsibilities is to set up authorizations to control the access to HR Cluster data. As a result, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Assign HR cluster data authorization to administrators

Authorization Object: HR Clusters

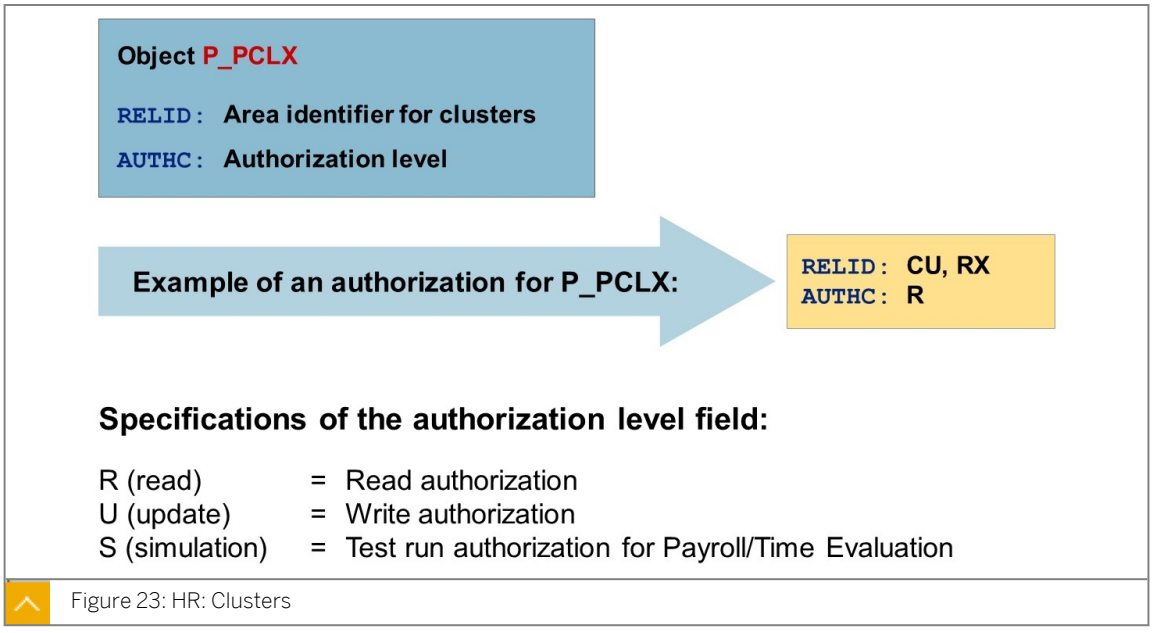

Figure 23: HR: Clusters

You can use the authorization object P_PCLX, *HR: Clusters*, during the authorization check for access to `PCLX` HR files (x = 1, 2, 3, 4) as long as these accesses are via the `PCLX` buffer (interface supported by HR).

The possible values for the area indicator are the fixed values of the `RELID_PCL` domain. The fixed values and definitions of what they mean are stored in the *T52RELID* table (transaction `PECLUSTER`).

LESSON SUMMARY

You should now be able to:

- Assign HR cluster data authorization to administrators

Unit 2
Lesson 7

Defining Customer-Specific HR Authorization Objects

LESSON OVERVIEW
This lesson outlines customer-specific authorization objects.

Business Example:

As a member of the authorization team, you are responsible for the set up of customer-specific authorization objects. As a result, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Define customer-specific HR authorization objects

Customer-Specific HR Authorization Objects

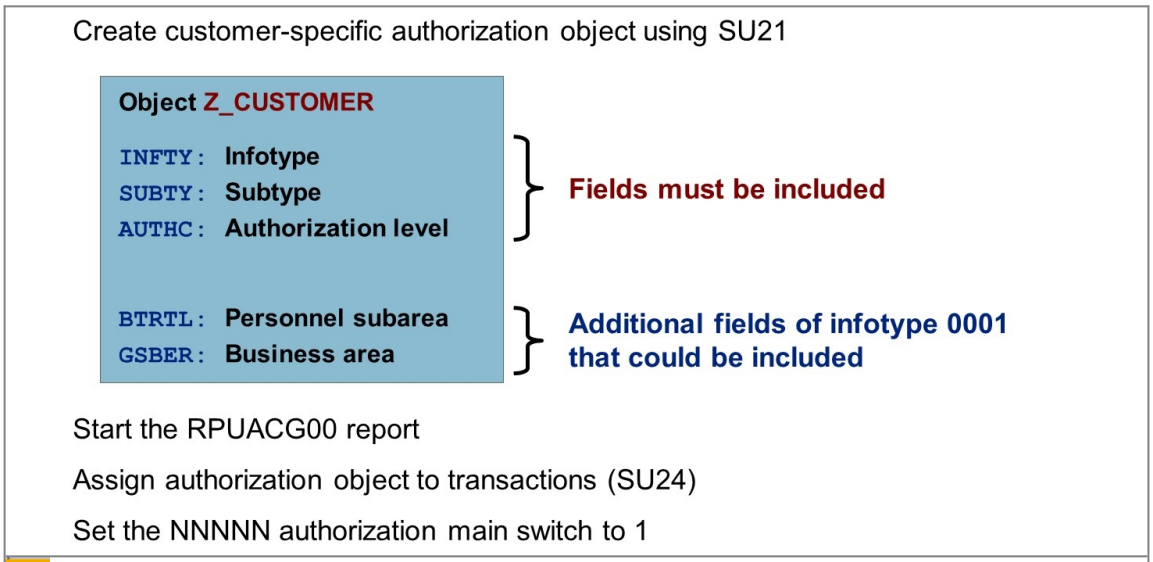

Figure 24: HR: Master Data - Customer-Specific Object

If you have requirements that cannot be met using the P_ORGIN and P_ORGXX authorization objects, you can include an authorization object in the authorization checks yourself. Ffor example, you want to build your authorization checks on additional fields of the Organizational Assignment infotype (0001) that are customer-specific,

Create the authorization object using transaction SU21, making sure you keep to the customer name range (Z/Y). To be able to use the new authorization object you created in the master data authorization check, the object must contain the INFTY, SUBTY, and AUTHC fields. You can use any other fields of the *Organizational Assignment* infotype (0001) as the

other fields. You can also use customer-specific additional fields provided they are CHAR or NUMC type fields.

After you have created the object, you must start the report RPUACG00. This report overwrites the MPPAUTZZ standard include with the code that is needed to evaluate the authorization object you created. Note: Technically speaking, this involves a modification. However, SAP fully supports this procedure. You should not have more maintenance work as a result of this modification.

If you use customer-specific authorization objects, you must maintain these objects in transaction SU24 (*Maintain Assignment of Authorization Objects to Transactions*) in the same way as you maintain the authorization objects P_ORGIN, P_ORGXX, and P_PERNR.

LESSON SUMMARY

You should now be able to:

- Define customer-specific HR authorization objects

Setting Up Authorization Verification

LESSON OVERVIEW
This lesson outlines the asymmetrical and symmetrical double verification principles and how they are used to ensure data is processed according to company procedures.

Business Example:

As a member of the authorizations team, you are responsible for the set up of administrator authorizations to ensure company procedures are followed when infotype information is processed by administrators. In some instances, two administrators are required to process infotype data. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline the asymmetrical double verification principle
- Outline the symmetrical double verification principle
- Set up a double verification for administrators

Asymmetrical Double Verification Principle

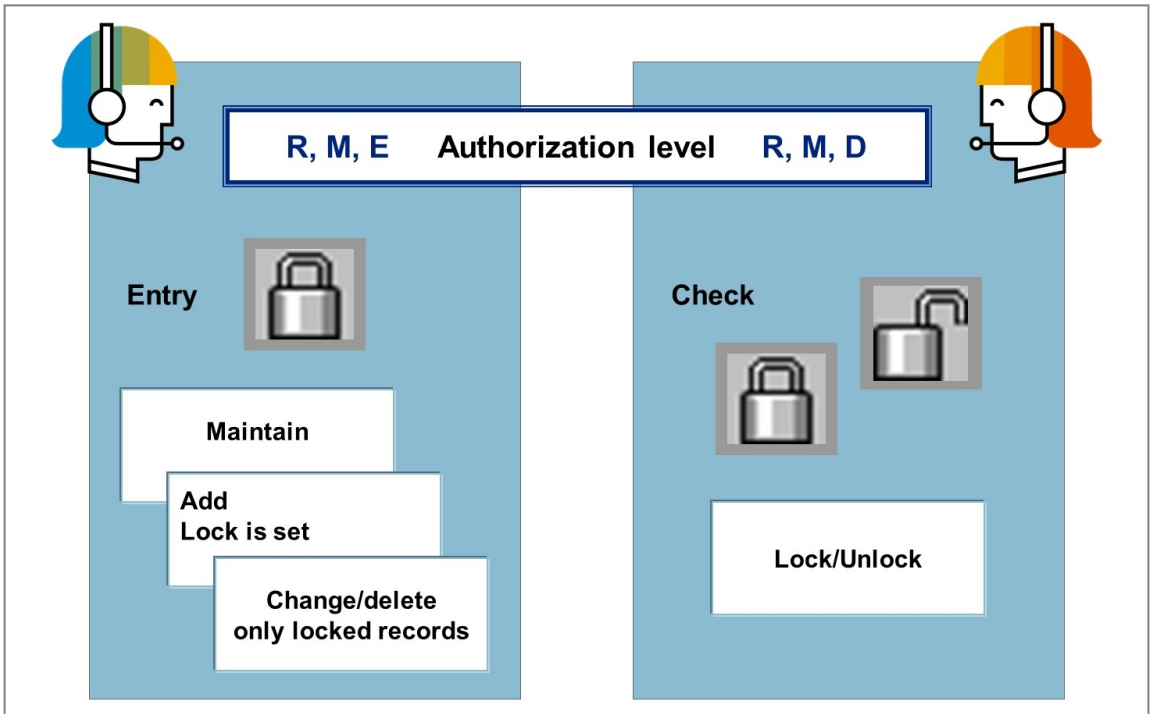

Figure 25: Asymmetrical Double Verification Principle

In this procedure, two users are always required to be able to create or change an infotype's data. The users **do not have the same authorizations**, which is why the process is called asymmetrical. User A is granted authorizations with the authorization level E (“enqueue”), R (“read”) and M (“matchcode”) for the P_ORGIN (or P_ORGXX) authorization object instead of complete write authorizations (authorization level W or *). These authorizations allow the user to create, change or delete locked records only.

User B is granted authorizations with the authorization level D (“dequeue”), R and M for the authorization object P_ORGIN (or P_ORGXX) instead of complete write authorizations. These authorizations allow the user to unlock locked records (or lock unlocked records) only.

New data is entered by user A and unlocked by user B. Existing data can be changed in two ways: User B locks the data, user A changes the data, and user B unlocks the data again. Alternatively, user A creates a locked copy from the unlocked data and changes this copy. User B then unlocks the data. To delete unlocked data, user B locks the data, which is then deleted by user A.

In this process, user A is always responsible for entering and changing data and user B for approving the changes.

Symmetrical Double Verification Principle

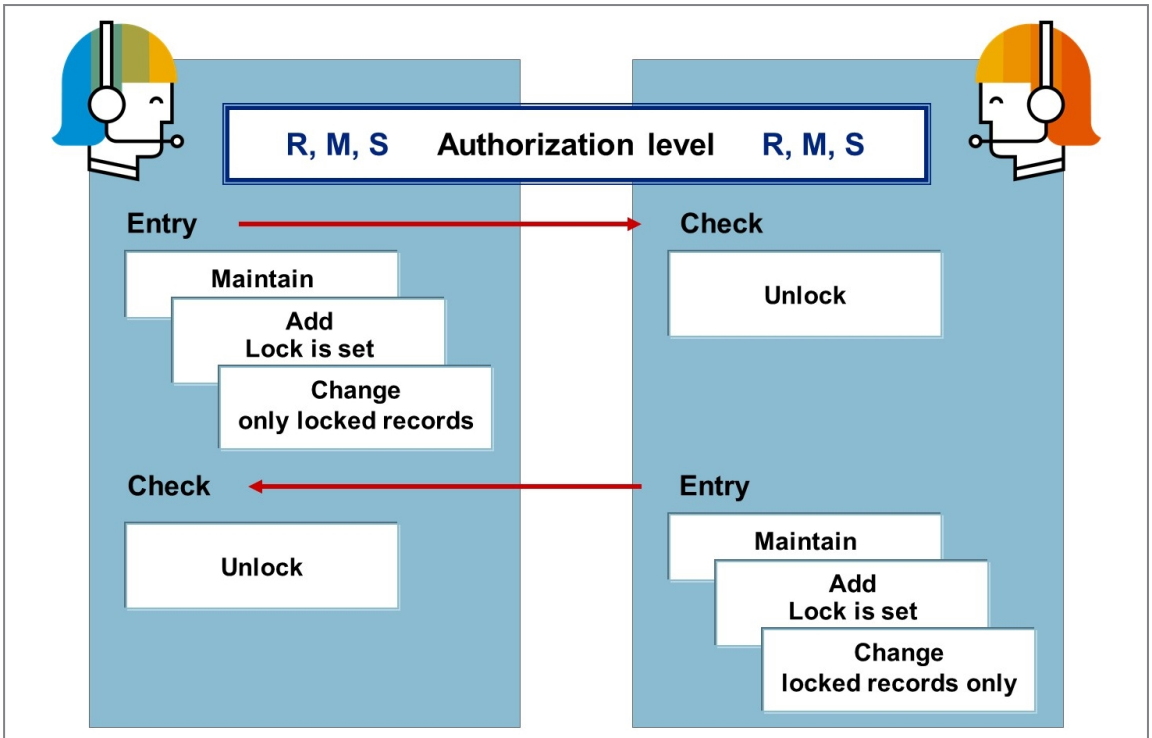

Figure 26: Symmetrical Double Verification Principle

In this procedure, two users are always required to be able to create or change an infotype's data. The users have the **same authorizations** for this. The procedure is as follows: Both users are granted authorizations with the authorization level S (“symmetrical”), R (“read”) and M (“matchcode”) for the P_ORGIN (or P_ORGXX) authorization object instead of full write authorizations (authorization level W or *). These authorizations allow each user to create locked data records, change locked data records, and relock unlocked data records. In addition, each user can unlock data as long as he or she is not the last person to have changed the locked data. Neither user can delete data.

New data is created by user A (or user B) and locked by user B (or user A).

To change existing data: user A (or user B) locks and changes the data and user B (or user A) unlocks the data.

Another user must be consulted to delete existing data.

Double Verification Principle

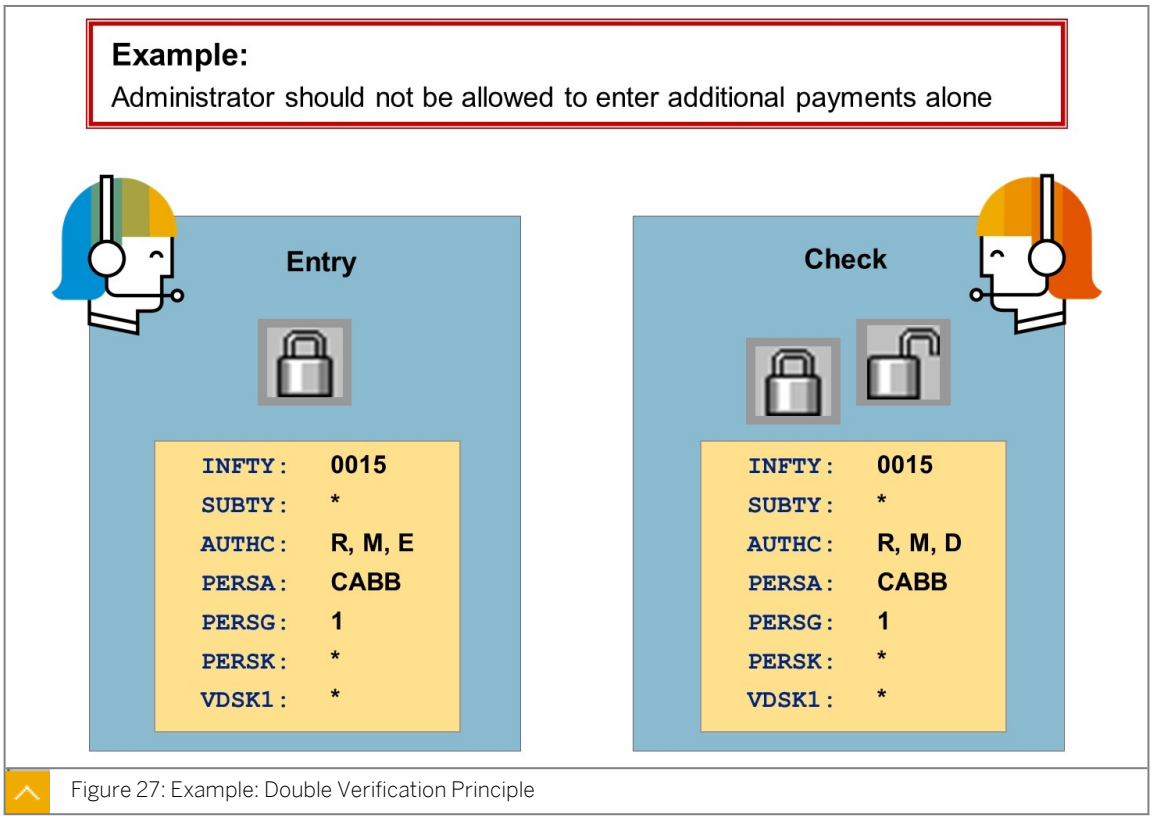

Figure 27: Example: Double Verification Principle

You want to ensure that the *Additional Payments* infotype (0015) can only be edited by two administrators together. To achieve this, you want to set up the asymmetrical double verification principle where one of the administrators is responsible for recording the data and the other administrator is responsible for controlling the process.

The administrator responsible for recording the data requires the authorization for the P_ORGIN authorization object shown on the left in the figure Example: Double Verification Principle. The administrator responsible for controlling the data requires the authorization on the right in the figure Example: Double Verification Principle.

LESSON SUMMARY

You should now be able to:

- Outline the asymmetrical double verification principle
- Outline the symmetrical double verification principle
- Set up a double verification for administrators

Learning Assessment

1. Which of the following statements about an authorization object is true?

   Choose the correct answer.

   - ☐ **A** An authorization object groups up to 10 authorization fields that are checked in an OR relationship.
   - ☐ **B** An authorization object groups up to 20 authorization fields that are checked in an AND relationship.
   - ☐ **C** An authorization object groups up to 10 authorization fields that are checked in an AND relationship.
   - ☐ **D** An authorization object groups up to 20 authorization fields that are checked in an OR relationship.

2. The authorization check for the object HR: Master Data – Personnel Number Check is performed as a rule.

   Determine whether this statement is true or false.

   - ☐ True
   - ☐ False

3. The master data authorization check differentiates between an alternative and an additional version. Which of the following statements apply to the additional check?

   Choose the correct answer.

   - ☐ **A** A check is performed on the authorizations for the objects HR: Master Data and HR: Personnel Number Check.
   - ☐ **B** A check is performed on the authorizations for the objects HR: Master Data or HR: Master Data – Extended Check.
   - ☐ **C** First, a check is performed on the authorizations for HR: Master Data. If the result of this check is positive, a further check based on HR: Master Data – Extended Check is performed.
   - ☐ **D** First, a check is performed on the authorizations for HR: Personnel Number Check. If the result of this check is positive, a further check based on HR: Master Data is performed.

4. In which of the following cases will the system use the authorization object HR: Master Data – Personnel Number Check?

   Choose the correct answer.

   - ☐ A When a user does not have an organizational personnel number.
   - ☐ B When you want to assign users different authorizations for accessing their own personnel numbers.
   - ☐ C When a user does not have a communications infotype 0105 with subtype 0001.

5. Which of the following statements about authorization main switches are correct?

   Choose the correct answers.

   - ☐ A You can use these switches to adjust the behavior of the authorization check on HR infotypes to meet your requirements.
   - ☐ B You can use one authorization main switch at a time.
   - ☐ C You can use these switches to specify the switch settings at the client level differently.
   - ☐ D These switches are stored in table T77S0 under the group name AUTSW.

6. Reference users are used to assign identical authorizations to Internet users.

   Determine whether this statement is true or false.

   - ☐ True
   - ☐ False

7. Which of the following SAP E-Recruiting roles can be changed, but must not be deleted?

   Choose the correct answers.

   - ☐ A Manager
   - ☐ B Recruiter
   - ☐ C Data entry manager
   - ☐ D Decision maker

8. When creating your own user roles, you must create customer roles in the SAP namespace.

   Determine whether this statement is true or false.

   - ☐ True
   - ☐ False

9. The check for the Personnel Planning object can be deactivated in the authorization main switch.

   Determine whether this statement is true or false.

   ☐ True

   ☐ False

10. No manual changes should be made in the authorization for the HR: Transaction Code object.

    Determine whether this statement is true or false.

    ☐ True

    ☐ False

11. For which authorization object do you need authorization to access payroll results?

    Choose the correct answer.

    ☐ A HR: All

    ☐ B HR: Clusters

    ☐ C HR: Master Data

12. You can add fields from any infotypes to a customer-specific authorization object.

    Determine whether this statement is true or false.

    ☐ True

    ☐ False

13. Determine which double verification procedure to use for this business example, symmetrical or asymmetrical.

    Choose the correct answers.

    ☐ A In this procedure, two users are always required to be able to enter or change data of an infotype.

    ☐ B The double verification principle compensates an oversight by a user.

    ☐ C The double verification principle has a symmetrical and an asymmetrical version.

Learning Assessment - Answers

1. Which of the following statements about an authorization object is true?

   Choose the correct answer.

   - [ ] A An authorization object groups up to 10 authorization fields that are checked in an OR relationship.
   - [ ] B An authorization object groups up to 20 authorization fields that are checked in an AND relationship.
   - [x] C An authorization object groups up to 10 authorization fields that are checked in an AND relationship.
   - [ ] D An authorization object groups up to 20 authorization fields that are checked in an OR relationship.

   Correct. An authorization object groups up to 10 authorization fields that are checked in an AND relationship.

2. The authorization check for the object HR: Master Data – Personnel Number Check is performed as a rule.

   Determine whether this statement is true or false.

   - [ ] True
   - [x] False

   Correct. The statement is not correct.

3. The master data authorization check differentiates between an alternative and an additional version. Which of the following statements apply to the additional check?

   Choose the correct answer.

   ☐ A A check is performed on the authorizations for the objects HR: Master Data and HR: Personnel Number Check.

   ☐ B A check is performed on the authorizations for the objects HR: Master Data or HR: Master Data – Extended Check.

   ☒ C First, a check is performed on the authorizations for HR: Master Data. If the result of this check is positive, a further check based on HR: Master Data – Extended Check is performed.

   ☐ D First, a check is performed on the authorizations for HR: Personnel Number Check. If the result of this check is positive, a further check based on HR: Master Data is performed.

   Correct. First, a check is performed on the authorizations for HR: Master Data. If the result of this check is positive, a further check based on HR: Master Data – Extended Check is performed.

4. In which of the following cases will the system use the authorization object HR: Master Data – Personnel Number Check?

   Choose the correct answer.

   ☐ A When a user does not have an organizational personnel number.

   ☒ B When you want to assign users different authorizations for accessing their own personnel numbers.

   ☐ C When a user does not have a communications infotype 0105 with subtype 0001.

   Correct. The system will use the authorization object HR: Master Data – Personnel Number Check, when you want to assign users different authorizations for accessing their own personnel numbers.

5. Which of the following statements about authorization main switches are correct?

   Choose the correct answers.

   [X] A You can use these switches to adjust the behavior of the authorization check on HR infotypes to meet your requirements.

   [ ] B You can use one authorization main switch at a time.

   [X] C You can use these switches to specify the switch settings at the client level differently.

   [X] D These switches are stored in table T77S0 under the group name AUTSW.

   Correct. You can use these switches to adjust the behavior of the authorization check on HR infotypes to meet your requirements, you can use these switches to specify the switch settings at the client level differently, and these switches are stored in table T77S0 under the group name AUTSW.

6. Reference users are used to assign identical authorizations to Internet users.

   Determine whether this statement is true or false.

   [X] True

   [ ] False

   Correct. Reference users are used to assign identical authorizations to Internet users.

7. Which of the following SAP E-Recruiting roles can be changed, but must not be deleted?

   Choose the correct answers.

   [X] A Manager

   [X] B Recruiter

   [ ] C Data entry manager

   [X] D Decision maker

   Correct. The following SAP E-Recruiting roles can be changed, but must not be deleted: Manager, Recruiter, and Decision maker

8. When creating your own user roles, you must create customer roles in the SAP namespace.

   Determine whether this statement is true or false.

   [ ] True

   [X] False

   Correct. The statement is not correct.

9. The check for the Personnel Planning object can be deactivated in the authorization main switch.

   Determine whether this statement is true or false.

   ☐ True

   ☒ False

   Correct. The check for this object cannot be deactivated in the authorization main switch with the switch ORGPD. The switch ORGPD lets you control whether the structural authorization checks are to be performed in Personnel Administration.

10. No manual changes should be made in the authorization for the HR: Transaction Code object.

    Determine whether this statement is true or false.

    ☒ True

    ☐ False

    Correct. No manual changes should be made in the authorization for the HR: Transaction Code object.

11. For which authorization object do you need authorization to access payroll results?

    Choose the correct answer.

    ☐ **A** HR: All

    ☒ **B** HR: Clusters

    ☐ **C** HR: Master Data

    Correct. You need maintained authorizations in the authorization object: HR: Clusters.

12. You can add fields from any infotypes to a customer-specific authorization object.

    Determine whether this statement is true or false.

    ☐ True

    ☒ False

    Correct. You can only add fields from the Organizational Assignment infotype (0001) to a customer-specific authorization object.

13. Determine which double verification procedure to use for this business example, symmetrical or asymmetrical.

    Choose the correct answers.

    [X] A In this procedure, two users are always required to be able to enter or change data of an infotype.

    [ ] B The double verification principle compensates an oversight by a user.

    [X] C The double verification principle has a symmetrical and an asymmetrical version.

    Correct. Symmetrical double verification means that the two users have the same authorizations, while with asymmetrical double verification, one user may only enter data but not check it.

UNIT 3 Indirect Role Assignment

Lesson 1

UNIT OBJECTIVES

- Outline organizational management authorizations
- Outline user assignments
- Compare user authorization assignments

Unit 3
Lesson 1

Assigning Roles Indirectly

LESSON OVERVIEW
This lesson outlines organizational management authorizations, how users are assigned, and how to compare user assignments.

Business Example

As the authorizations administrator, you are responsible for the assignment of organizational management authorizations and user assignments. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline organizational management authorizations
- Outline user assignments
- Compare user authorization assignments

Organizational Management Authorization Objects

Authorizations in Organizational Management

- Problem
  - Maintaining direct role assignments to users can be very time consuming for large implementations.
  - If users in the company change department or function, you have to adjust their authorizations.
- Solution:
  - Create roles on the basis of organizational objects, for example positions in your company such as sales executive, accountant, administrative assistant, and so on.
  - Assign roles to your organizational plan. Users then inherit the authorizations according to their position in the organizational plan.

Indirect role assignment means that you do not assign the role to one or more users directly in transaction SU01, SU10, or PFCG. Instead, you link the role using Organizational Management to an organizational unit, job, position, and so on. This has the following advantages:

Replacement and Change

- If you assign roles to individual users directly, you have to adjust this assignment each time an employee's responsibilities change.

- If you base the assignment on positions, you do not have to adjust the agent assignment of roles.

Time-Dependent Planning for Reorganizations

- SAP Organizational Management enables you to plan and activate the validity and assignment of organizational objects according to the time frame available. You must schedule the program for updating user master records to ensure the profiles can be added or deleted in accordance with the changes to the organizational plan.

Comparing the User Master

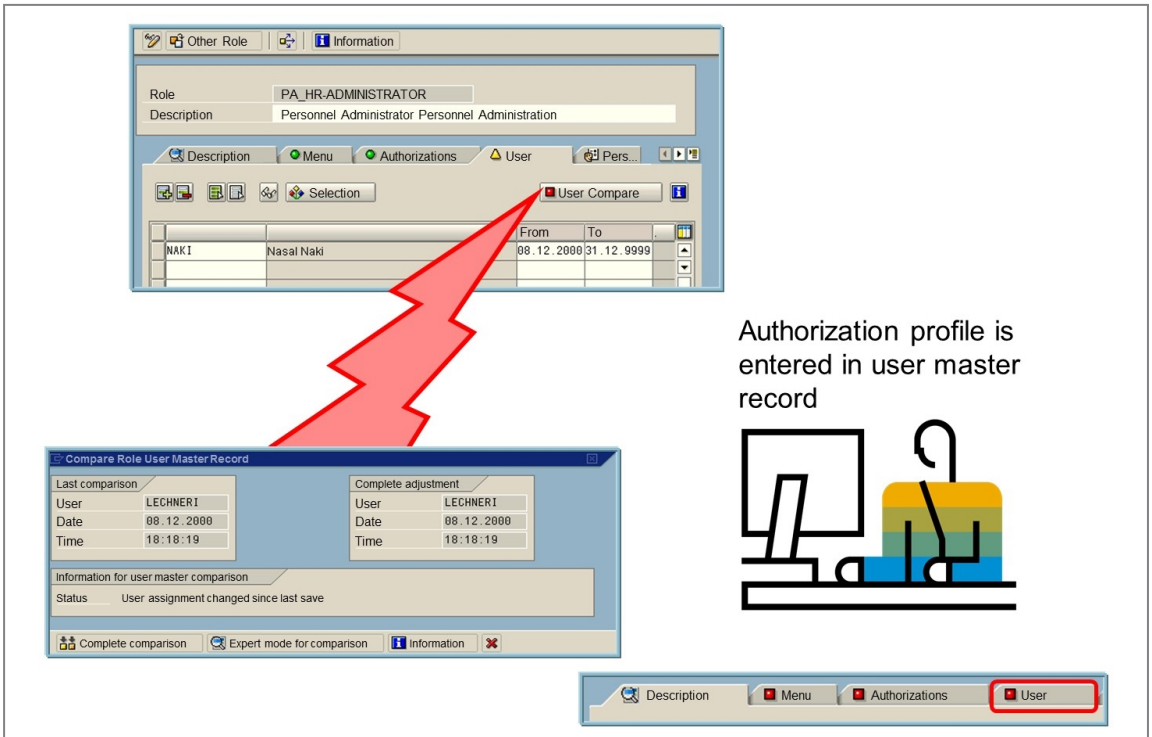

Figure 28: Comparing the User Master

For users to be authorized to execute the transactions contained in the menu tree of their role, their user master record must contain the profile for the corresponding roles.

You can start the user compare from role maintenance (on the *User* tab page, choose *User Compare*). As a result of the comparison, the role and the generated profile are entered in the user master record.

Caution:
Never enter generated profiles directly into the user master record (using transaction SU01, for example). During automatic user compare (by report PFCG_TIME_DEPENDENCY, for example), generated profiles are removed from user masters if they do not belong to the roles assigned to the user.

If you assign roles to users for a limited period of time only, you must perform a comparison at the beginning and at the end of the validity period. You are recommended to schedule the background job **PFCG_TIME_DEPENDENCY** in such cases.

User Assignment View of Authorizations

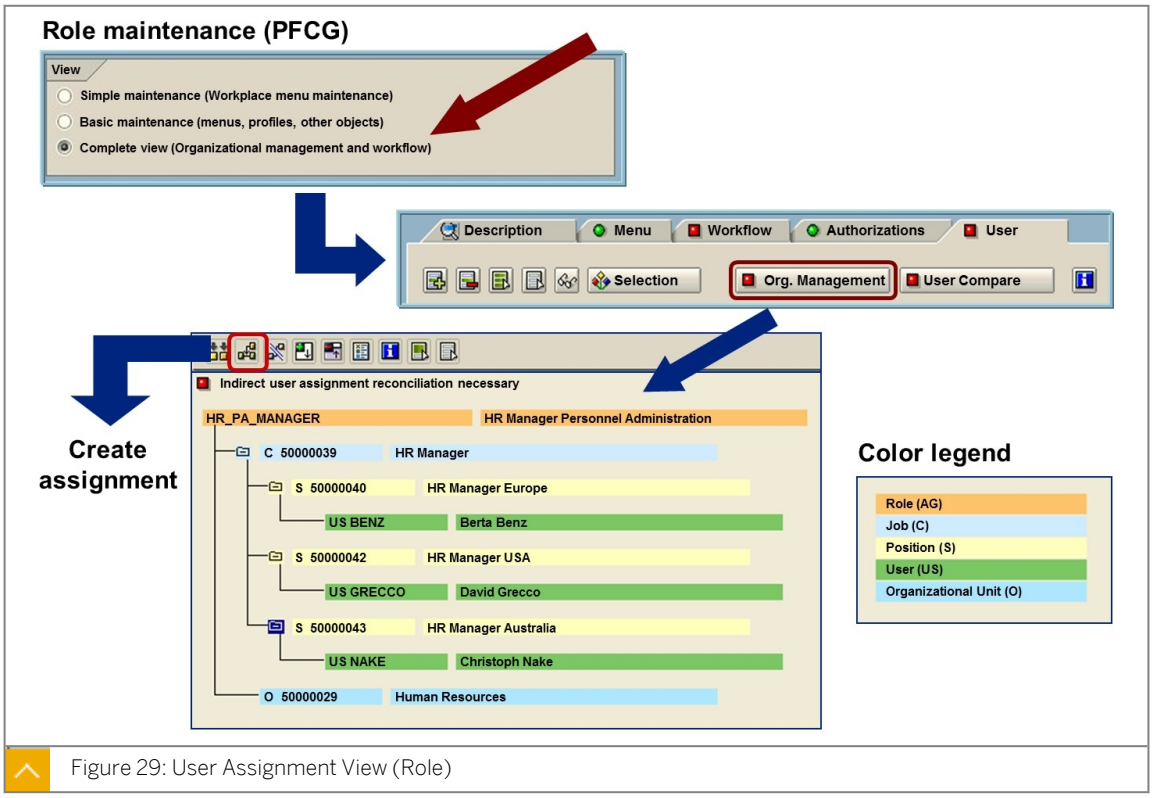

Figure 29: User Assignment View (Role)

To be able to assign components to your organizational plan, you must call role maintenance (PFCG) by choosing *Goto → Settings Overall View*.

Choose the *Organizational Mgmt.* button to go to the maintenance screen *Role: Maintain Agent Assignment*. The “indirect user assignments” that have already been maintained are displayed here.

When you are creating an assignment, if you select the agent type Position, you can assign users to a role using positions. One of the following prerequisites must be fulfilled:

1. The position is related to a person (P) whose user is entered in infotype 0105 *Communication*.

   OR

2. The position is related with a user (US).

You can define the following relationships by choosing *Create assignment*:

Role → Organizational unit/position/user/job/work center/person.

Indirect User Authorization Assignments

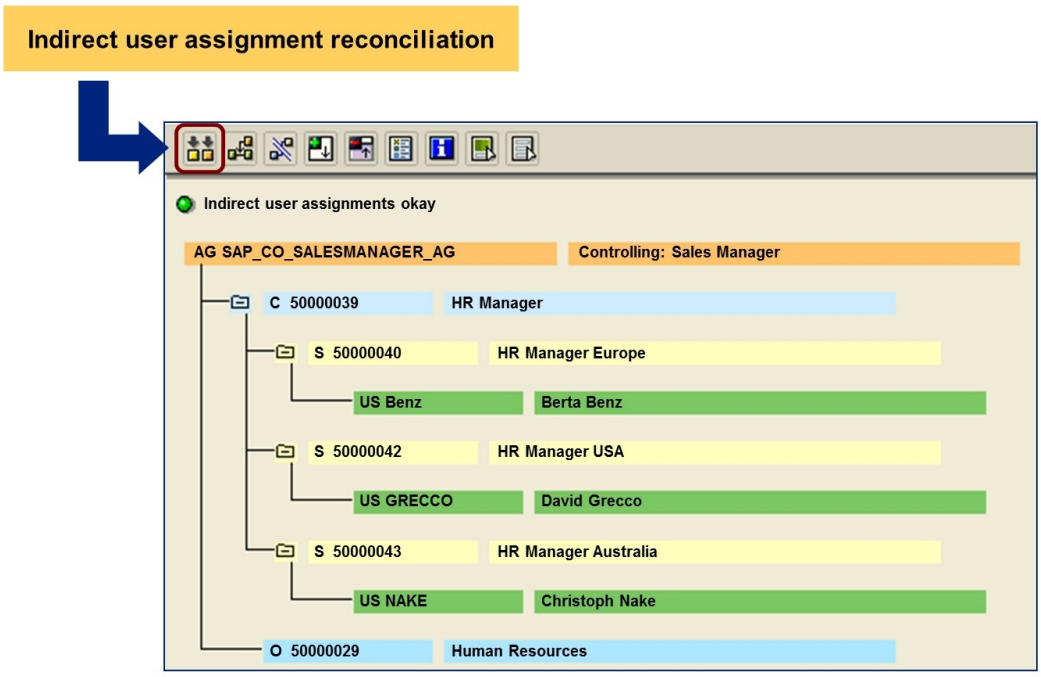

Figure 30: Compare Indirect User Assignment

If you choose *Indirect user assignment reconciliation*, the system reconciles the positions and the users assigned. Users that were newly added are entered, and user assignments that are no longer current are deleted.

During the reconciliation process, the users assigned on the basis of positions are entered as “indirect user assignments” for the role.

Since assignments in Organizational Management are time-dependent, you must take this time dependency into account when you assign users. This occurs during the reconciliation process when the relationship period is copied from Organizational Management for the indirect user assignments.

The status display of the button *Org.Management* indicates whether or not you have to update the indirect user assignments:

- Green:

  User assignments are up to date

- Red:

  User assignments are not up to date; the indirectly assigned users are not displayed in full on the tab page

  If you run a user master compare (refer to the figure titled Compare Indirect User Assignment), the *indirect user assignment* is automatically reconciled. The same applies if you run the PFCG_TIME_DEPENDENCY report.

Compare the User Master

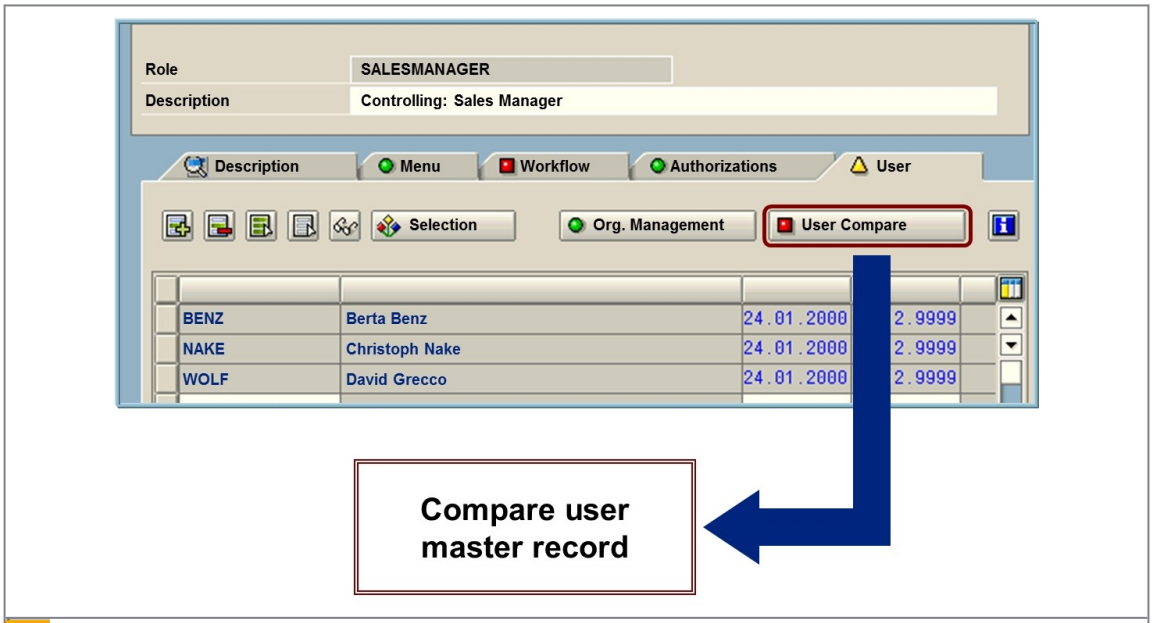

Figure 31: Compare the User Master

If you change the users assigned to the role or generate an appropriate authorization profile, you must compare the user masters (choose *User compare*). In this process, the system compares the authorization profiles with the user master records. This means that profiles that are no longer up-to-date are removed from the user master records, and the up-to-date profiles are entered in the user master records.

Compare User Master Records

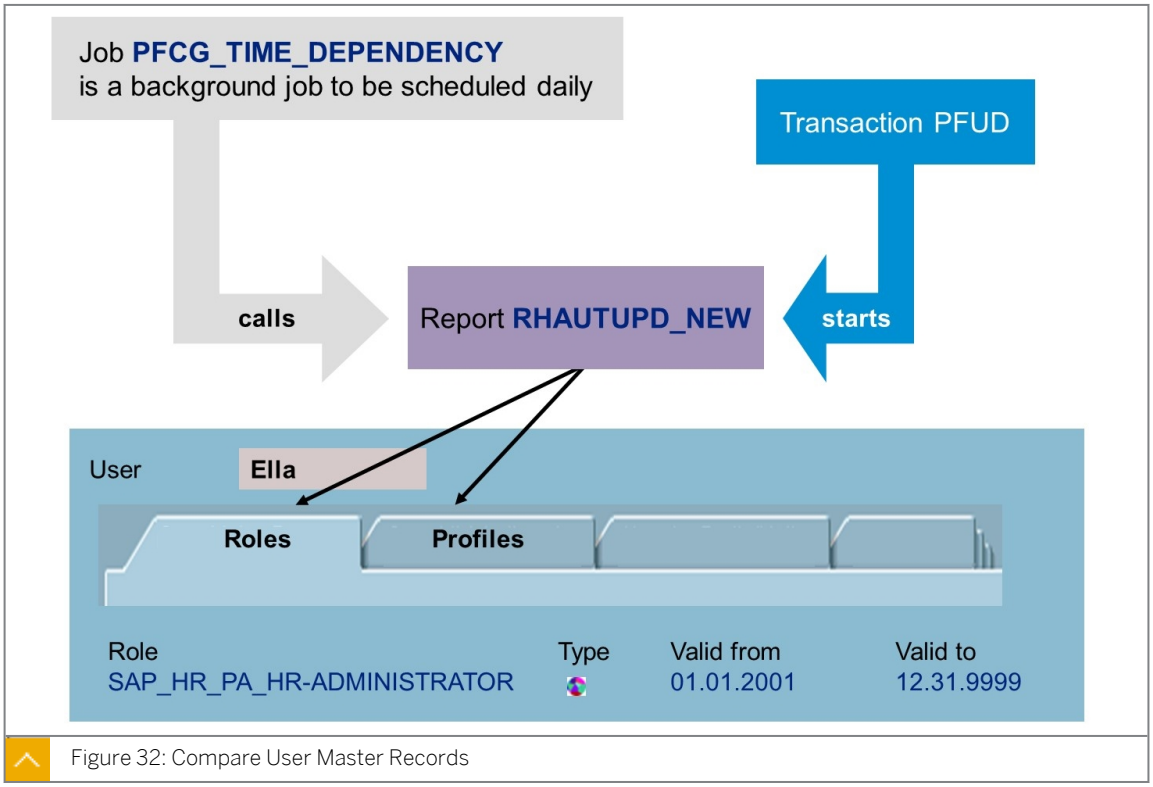

Figure 32: Compare User Master Records

You can specify a time limit when you assign roles to user master records. You **cannot** specify a time restriction for authorization profiles and their entries in the user master record.

To ensure that only the authorization profiles valid for a specific day are included in the user master record, you must perform a daily comparison. When you start report **RHAUTUPD_NEW**, a complete comparison of the user master records takes place for all roles. The authorizations in the user master records are updated. The profiles with invalid user assignments are removed from the user master record. The authorization profiles for valid user assignments for the role are entered.

There are two ways to run the comparison:

1. If you run job**PFCG_TIME_DEPENDENCY** nightly as a background job, the authorization profiles in the user master record are up to date every morning (if the job runs without errors).
2. Use transaction **PFUD**, *User Master Data Reconciliation*. As administrator, you should run the transaction regularly for control purposes. This gives you the opportunity to manually correct any errors that occurred in the background.

You can specify whether HR Organizational Management should be included in the reconciliation (*Reconcile with HR Organizational Management)*.

LESSON SUMMARY
You should now be able to:

- Outline organizational management authorizations
- Outline user assignments
- Compare user authorization assignments

Learning Assessment

1. What does indirect role assignment mean?

2. What are the advantages of relating a role with a position?

Learning Assessment - Answers

1. What does indirect role assignment mean?

   Indirect role assignment means that you do not assign the role to one or more users directly in transaction SU01, SU10, or PFCG. Instead, you link the role using Organizational Management to an organizational unit, job, position, and so on. I

2. What are the advantages of relating a role with a position?

   Users then inherit the authorizations according to their position in the organizational plan.

UNIT 4 Period of Responsibility for Administrators

UNIT OBJECTIVES

- Outline the connection of the period of responsibility to time logic
- Outline the process of system determination of the period of responsibility
- Outline the concept of tolerance times for authorization checks
- Outline time dependency of the authorization check
- Outline read access time logic
- Outline write access time logic
- Describe the application of time-dependent logic
- Lock the data using the time-dependent authorization

Unit 4
Lesson 1

Determining the Period of Responsibility for Administrators

LESSON OVERVIEW
This lesson outlines the attributes of the period of responsibility and time logic for authorizations.

Business Example:

You are responsible for the maintenance of authorizations for HR data. In your company, administrators responsible for maintaining infotype data often transfer between various departments. You must ensure that administrators have the correct access to information according to their current assignment. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline the connection of the period of responsibility to time logic
- Outline the process of system determination of the period of responsibility
- Outline the concept of tolerance times for authorization checks
- Outline time dependency of the authorization check

Period of Responsibility and Time Logic

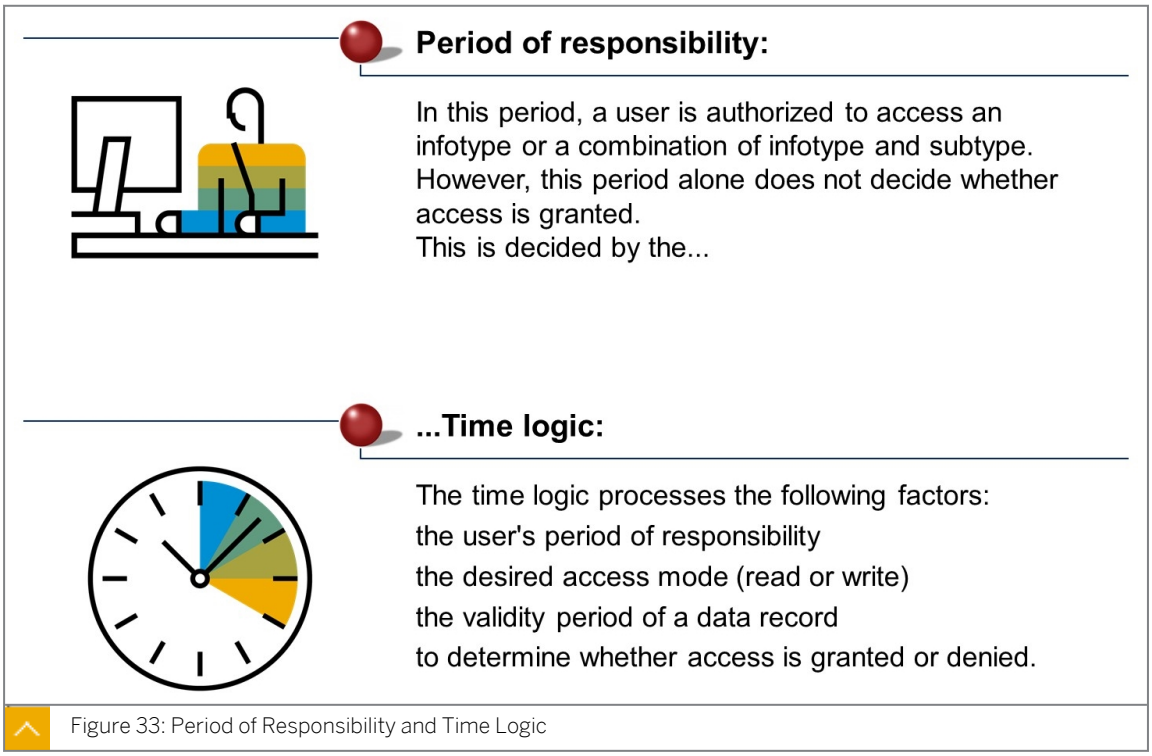

Figure 33: Period of Responsibility and Time Logic

The validity period of a data record may be only partly in a user's period of responsibility. For this reason, there is a time logic that decides the validity of the authorization.

Period Responsibility Determination

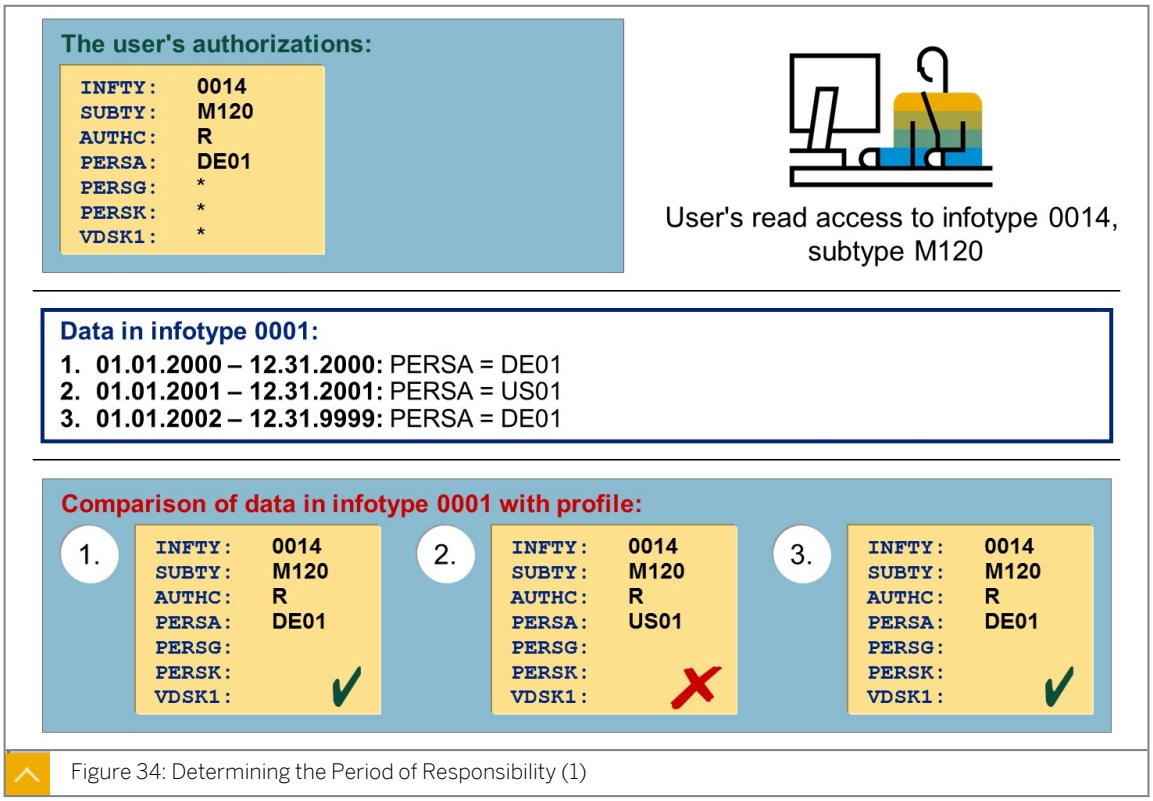

Figure 34: Determining the Period of Responsibility (1)

Process of determining the period of responsibility: First the system reads the organizational assignment of the personnel number (data records of the 0001 infotype).

Then an authorization check is performed for P_ORGIN for each organization assignment (data record of infotype 0001):

1. For 01/01/2000 – 12/31/2000:

   On the basis of the authorization in the profile, the authorization check is successful. The period lies within the period of responsibility.

2. For 01/01/2001 – 12/31/2001:

   The authorization does not permit access to PERSA = US01. The authorization check is unsuccessful and the period does not lie within the period of responsibility.

3. 01.01.2002 – 31.12.9999:

   On the basis of the authorization, the authorization check is successful. The period lies within the period of responsibility.

Period Responsibility Determination (2)

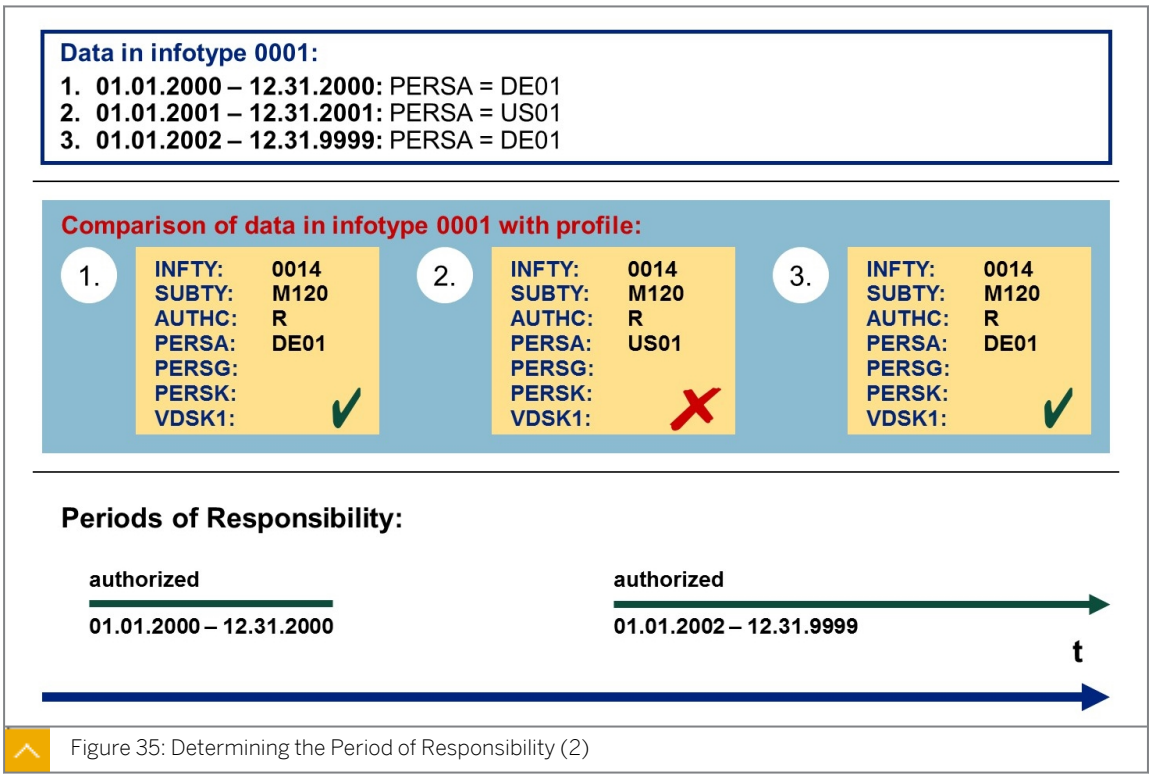

Figure 35: Determining the Period of Responsibility (2)

When all the organizational assignments of the personnel number have been evaluated, the period of responsibility is returned. If the period of responsibility is empty, “ *not authorized* ” is returned as the result. Otherwise, the result is “ *authorized* ”.

In this example, the period of responsibility consists of the periods January 1, 2000 to December 31, 2000 and January 1, 2002 to December 31, 9999.

Tolerance Time of the Authorization Check

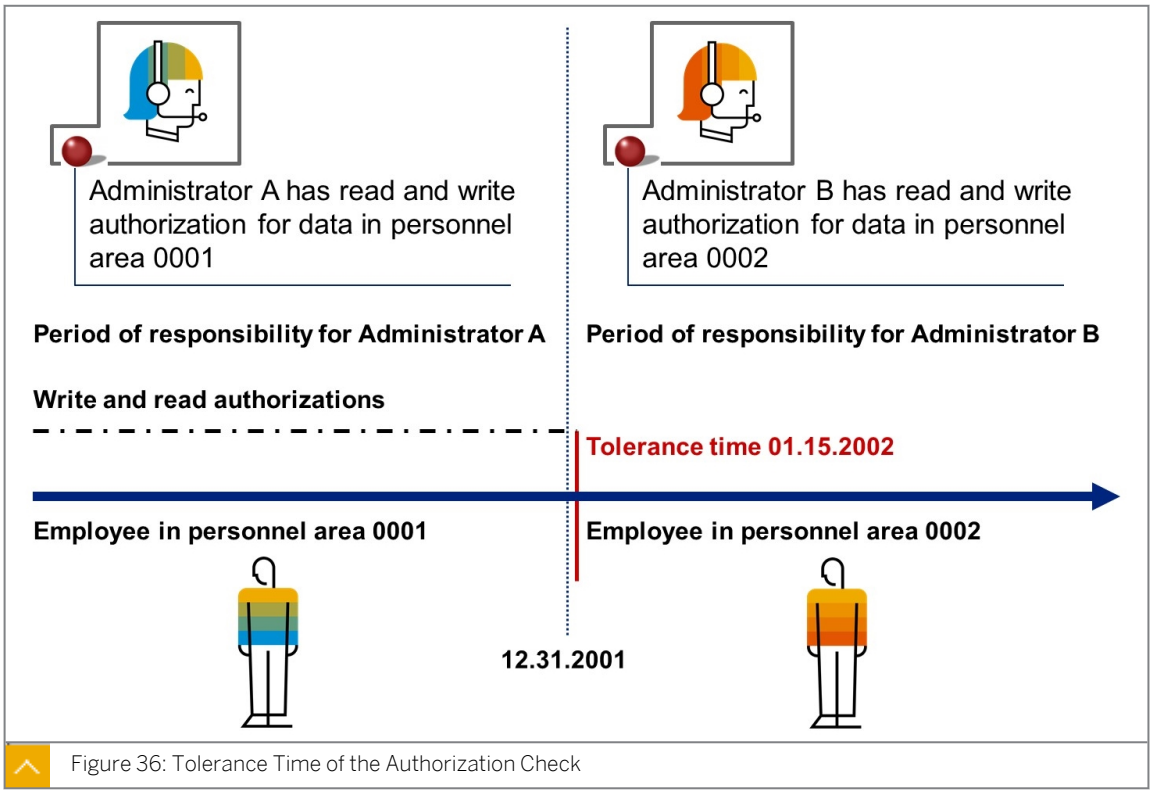

Figure 36: Tolerance Time of the Authorization Check

If the ADAYS authorization main switch is active, that is, if it contains a value greater than zero, the organizational reassignment of an employee, which results in the authorization of the administrator currently responsible for the employee being revoked, is delayed by the **tolerance time**. The tolerance time enables an administrator to make any necessary changes to the data of an employee after this employee has left the administrator's area of responsibility by providing a transition period in which the administrator still has access authorization to the data.

Hint:
You can make the setting using the OOAC transaction. In the standard system, ADAYS is set to **15**.

Time Dependency of the Authorization Check

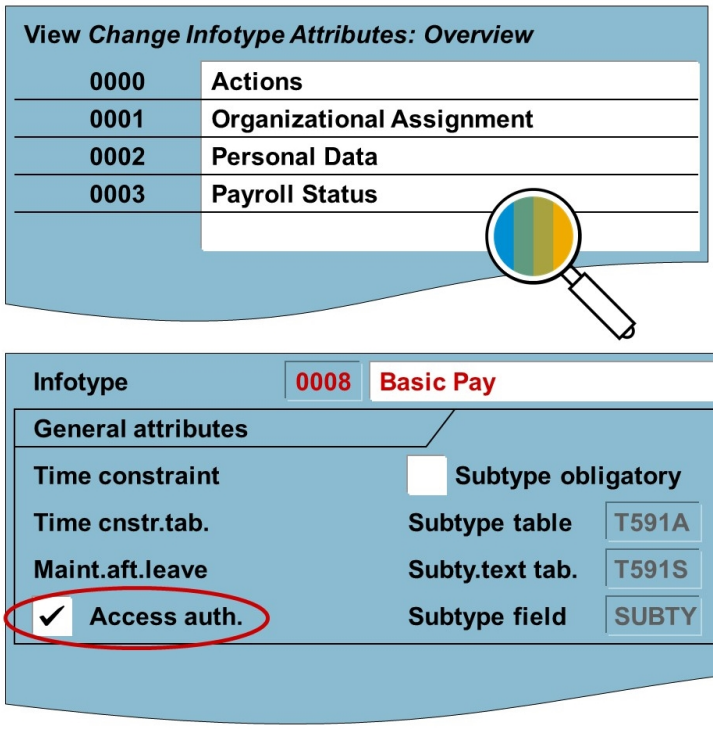

Figure 37: Time Dependency of the Authorization Check

If the access authorization indicator is not set in view T_582A, an administrator already has access to the relevant infotypes on the basis of his or her authorization profile if the person concerned had, has, or will have an organizational assignment at any time that falls in the administrator's responsibility according to his or her authorization profile.

If the indicator is set, the authorization check is dependent on the current date (system date).

The term period of responsibility is used in the following examples for the sake of simplicity: If at any given period a person has one (or more) organizational assignment(s) for which the administrator is responsible on the basis of his or her authorization profile, the entire validity period of the organizational assignment(s) is defined as the period of responsibility.

Flowchart: Period of Responsibility

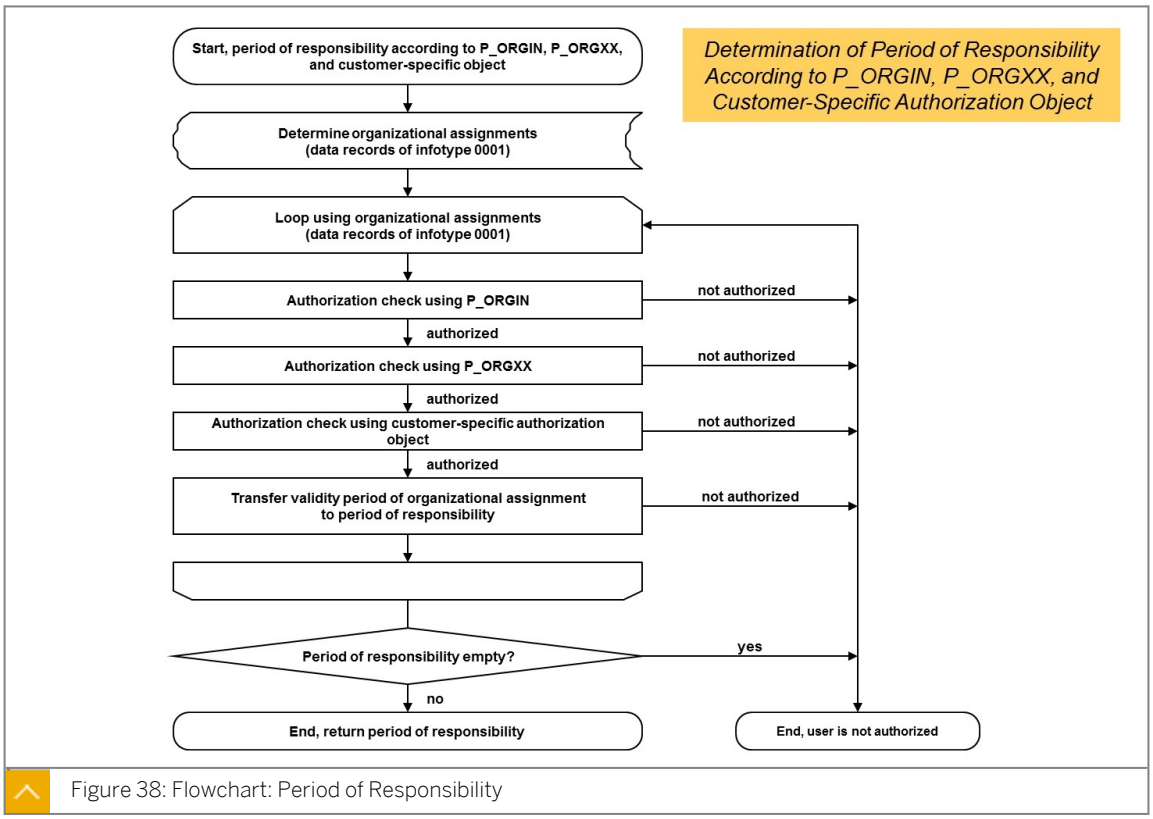

Figure 38: Flowchart: Period of Responsibility

The chart illustrates a typical flow for a determination of period of responsibility for the authorization objects P_ORIGIN, P_ORGXX and a customer specific authorization object.

LESSON SUMMARY

You should now be able to:

- Outline the connection of the period of responsibility to time logic
- Outline the process of system determination of the period of responsibility
- Outline the concept of tolerance times for authorization checks
- Outline time dependency of the authorization check

Unit 4
Lesson 2

Outlining Time Logic for Data Access

LESSON OVERVIEW
This lesson outlines how time logic is used when the system performs authorization checks.

Business Example:

As a member of the authorizations team, you are responsible for the maintenance of authorizations for time logic. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline read access time logic
- Outline write access time logic
- Describe the application of time-dependent logic
- Lock the data using the time-dependent authorization

Time Logic for Read Access

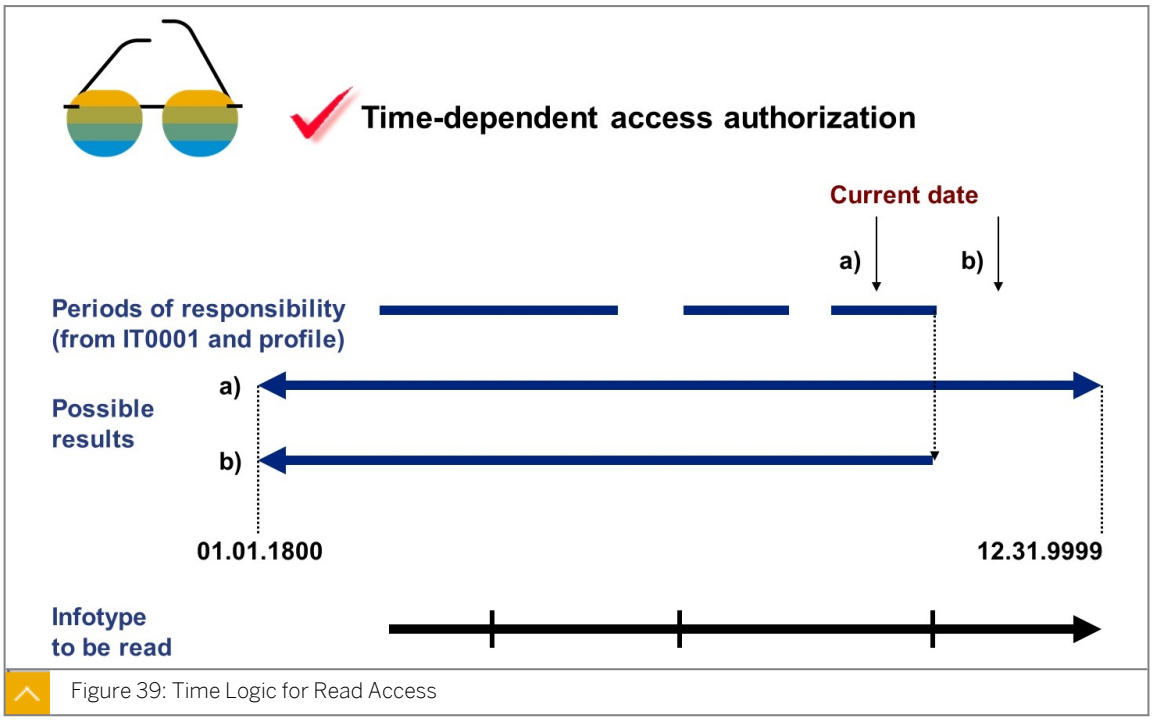

Figure 39: Time Logic for Read Access

The system determines whether the authorization check should be performed on a time-dependent basis or not. If the check should not be performed on a date-dependent basis, the

time logic check returns “ *authorized* ”. If the check should be performed on a date-dependent basis, the following steps are carried out:

The tolerance time and the end date of the period of responsibility are determined. The following results are possible:

1. If the current date (SY-DATUM) does not lie further than the tolerance time past the end date of the period of responsibility, the period 01/01/1800 to 12/31/9999 is set as the new period of responsibility.
2. If the current date lies further than the tolerance time past the end date of the period of responsibility, the period 01/01/1800 to the end date of the old period of responsibility is set as the new period of responsibility.

Finally, the check establishes whether the validity period BEGDA to ENDDA of the infotype intersects fully with the newly defined period of responsibility, that is, whether at least one day lies in both periods.

a) If the intersection is not empty, the time logic check returns “ *authorized* ”.

b) If the intersection is empty, the time logic check returns “ *not authorized* ”.

Time Logic for Write Access

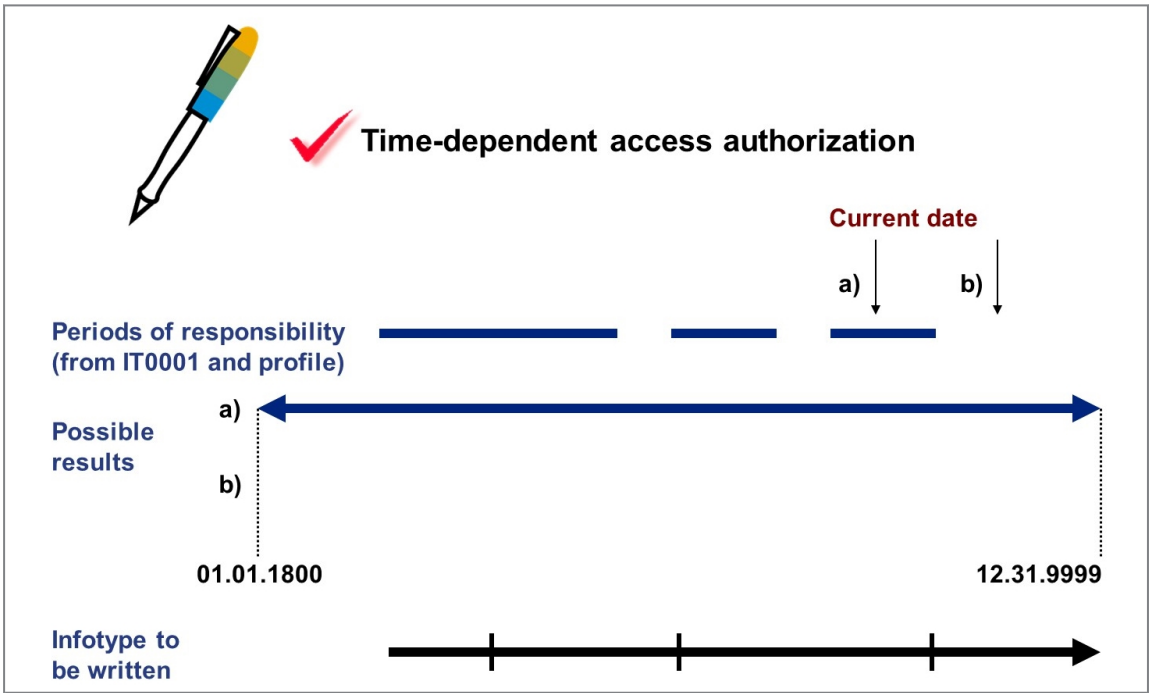

Figure 40: Time Logic for Write Access

The following steps are carried out: If the first day of the period of responsibility concurs with the first day of the organizational assignment (BEGDA of the first infotype record of infotype 0001, normally the date of the initial setting), the period of responsibility is extended to begin on January 1, 1800. This is necessary to ensure that users can access dates that are before the initial setting (for example, infotype 0002).

If the current date is within the period of responsibility or is not after the end of a responsibility interval by more than the tolerance time, the period January 1, 1800 to December 31, 9999 is set as the new period of responsibility.

If the current date is outside a responsibility interval and by more than the tolerance time after the end of each responsibility period, all responsibility intervals that are before the current date are deleted.

The check establishes whether the validity period BEGDA - ENDDA of the infotype to be written is completely within the newly defined period of responsibility:

1. If the validity period is within the period of responsibility, the time logic check returns " *authorized* ".
2. If the validity period is not within the period of responsibility, the time logic check returns " *not authorized* " and terminates.

Time-Dependent Logic

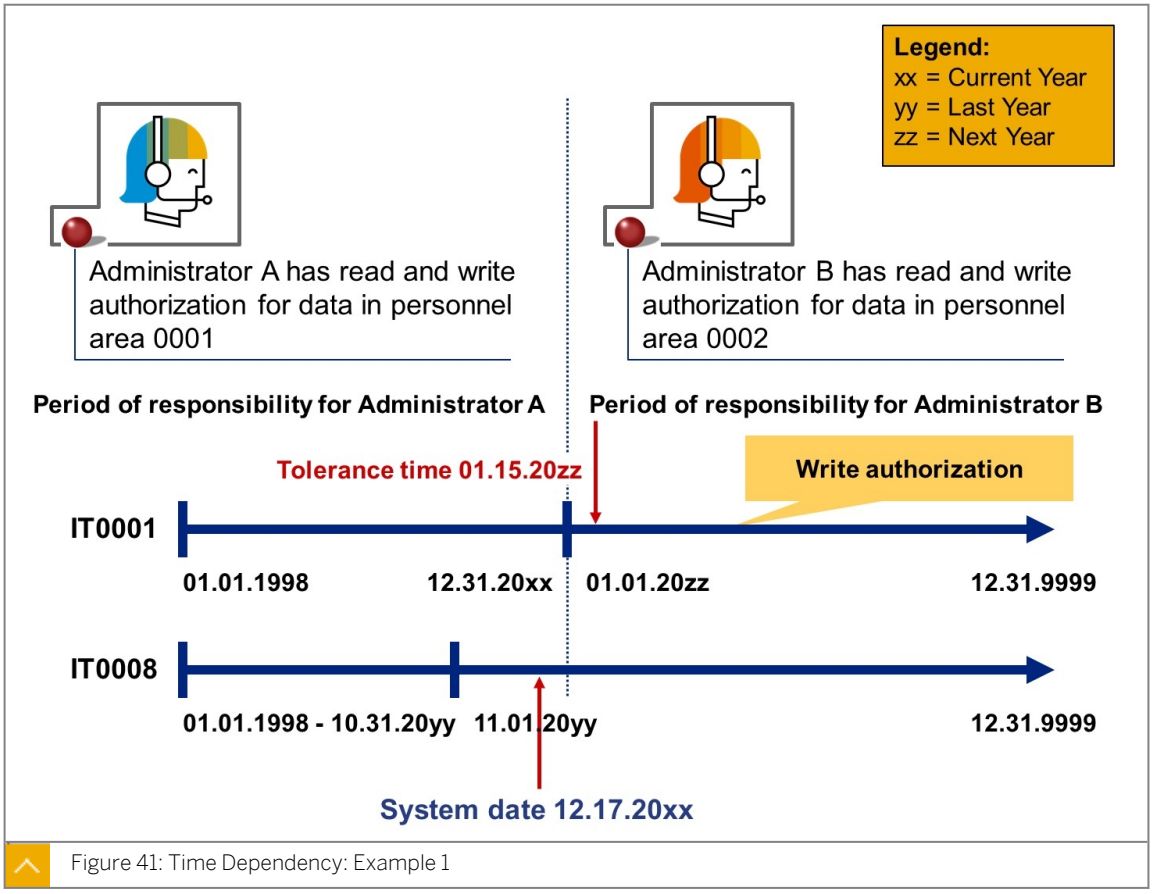

Figure 41: Time Dependency: Example 1

The following examples apply to this **situation**: An employee moves from personnel area 0001 to personnel area 0002 on January 1, 20xx (xx represents the year). Administrator A is responsible for personnel area 0001, administrator B for personnel area 0002.

Example 1:

The period of responsibility begins in the future:

If administrator B has write authorization for the corresponding infotype/subtype, this authorization is also valid for all infotype records with a validity period contained in the period of responsibility. In this example, an authorization exists for the record of infotype 0001 with the start date January 1, 20xx.

A read authorization exists for all infotype records with a validity period that overlaps with the period of responsibility or with a start date that is before the period of responsibility. In the example, administrator B has read authorization for both records of infotype 0008.

Time-Dependent Logic: Example 2

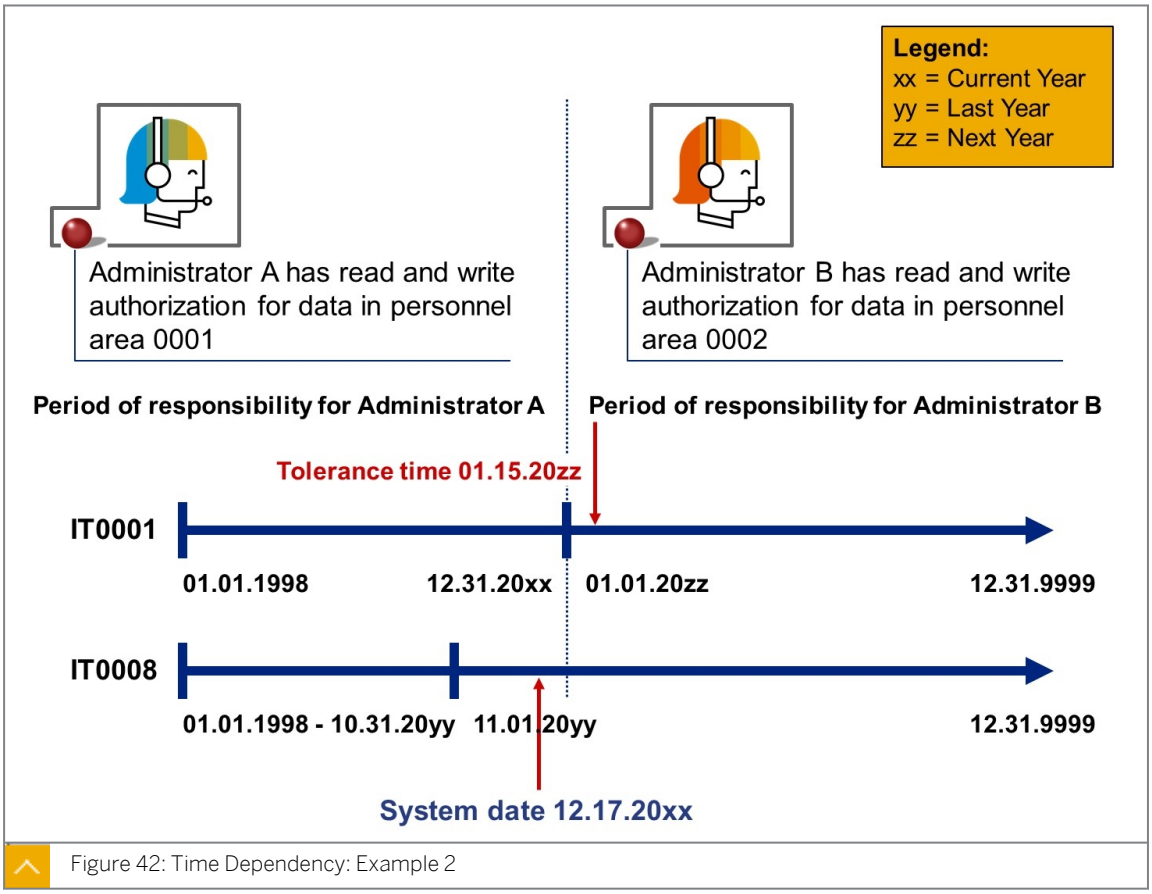

Figure 42: Time Dependency: Example 2

Example 2:

The period of responsibility begins before the current date. The end of the period of responsibility is before the current date by a maximum of a specified tolerance time.

In this case, a write or read authorization is extended to cover each period. This means that there are no restrictions on the authorization of the administrator A currently responsible with regard to the validity period of the corresponding infotype records.

Time-Dependent Logic: Example 3

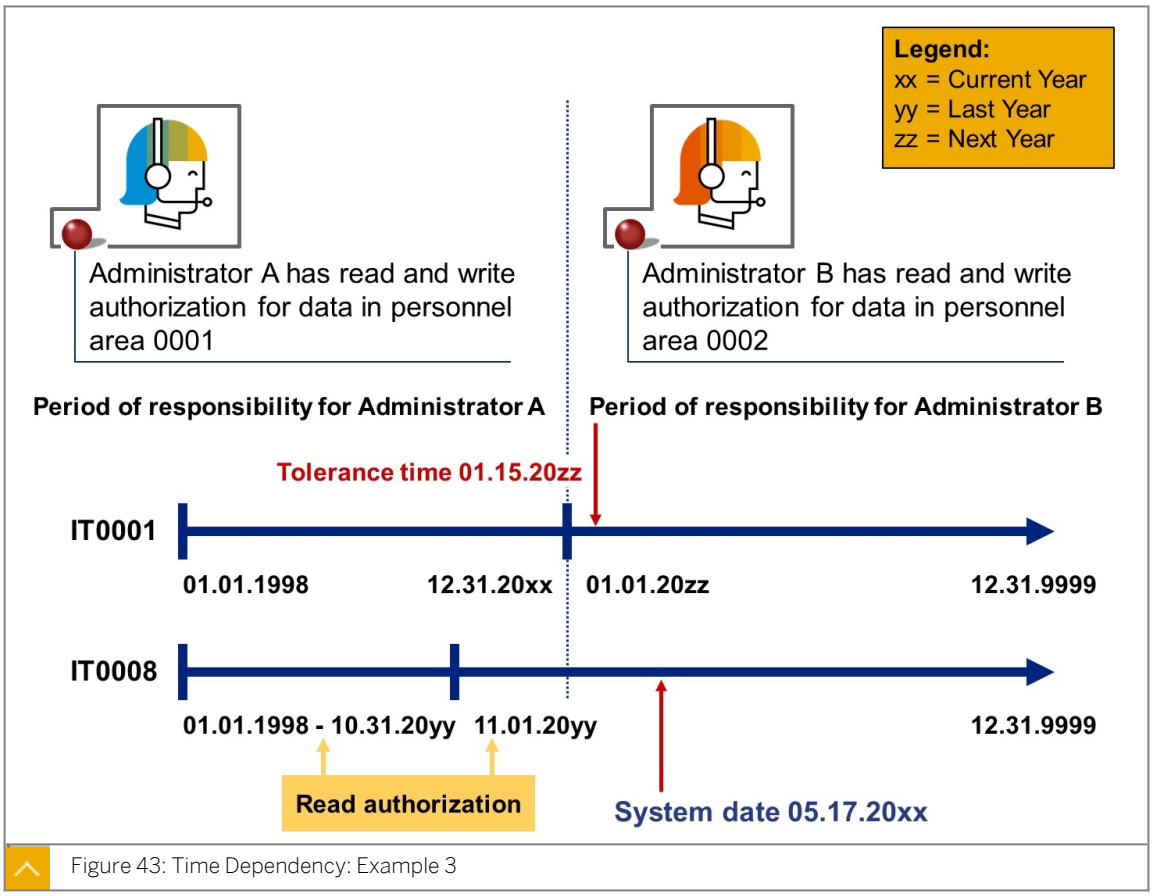

Figure 43: Time Dependency: Example 3

Example 3:

The period of responsibility ends in the past. The end of the period of responsibility, postponed for the length of the tolerance time, is also before the current date.

In this case, administrator A no longer has write authorization. Read authorization exists for the infotype records with a validity period that overlaps with the period of responsibility. In the example, administrator A has read authorization for both records of infotype 0008.

Flowchart: Time Dependent Logic

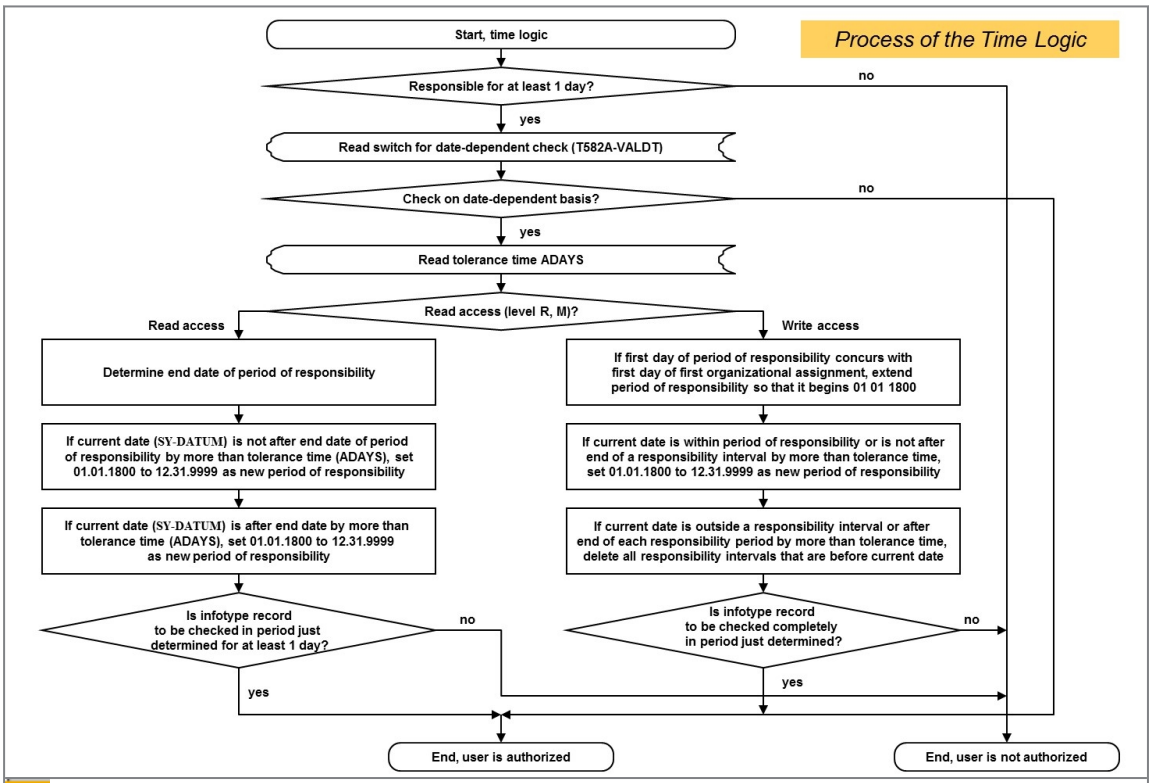

Figure 44: Flowchart: Time Dependent Logic

The flowchart illustrates a process of time logic.

Time Dependent Blocking of Data

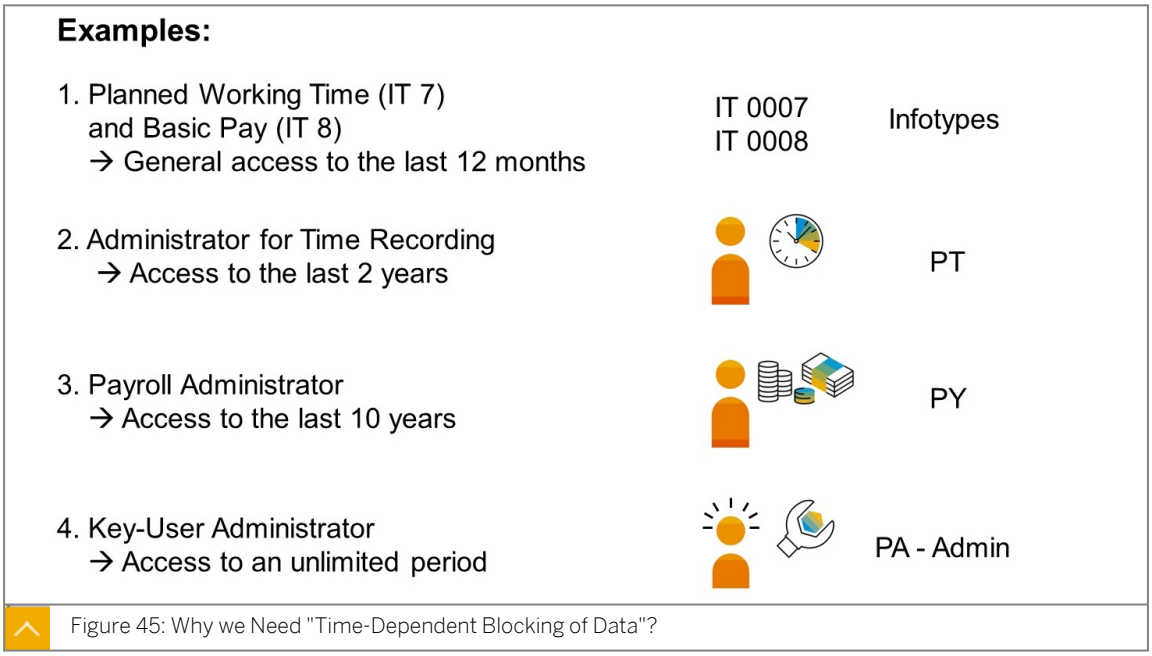

Figure 45: Why we Need "Time-Dependent Blocking of Data"?

Users can access HR data as a result of their direct or structural authorizations. However, if the data is no longer actively used, it might be necessary to protect it from further access.

This is the case when you no longer require the data for business purposes but cannot destroy it for other reasons.

To block users from the accessing data in the past in a time-dependent manner, you can enhance the SAP standard authorization check by customer-specific authorization checks. By changing the access authorizations, you can remove the access to personal data in the past so it cannot be used or changed. When doing so, take into consideration that different user role required different authorization time periods.

Examples:

1. In the past, all administrators required access authorization for infotype data 0007 (planned working time) and 0008 (basic pay).

2. In addition, a time data administrator must be able to display data from the time management infotype, such as 0007 (planned working time), 2 years in the past.

3. In addition, a payroll administrator must be able to display data from the payroll infotype, such as 0008 (basic pay), 10 years in the past.

4. Individual key user administrators may need unlimited access to employee data records.

By defining the authorization period, you can restrict the access to data in the past in a time-dependent manner, based on the system date. To do so, you define a minimum authorization period based on the type of data (infotype and subtypes) and the country grouping. You can enhance these minimum authorization periods for individual user roles and assign them to the corresponding roles (Authorization Object Authorization Time Periods for HR Master Data P_DURATION).

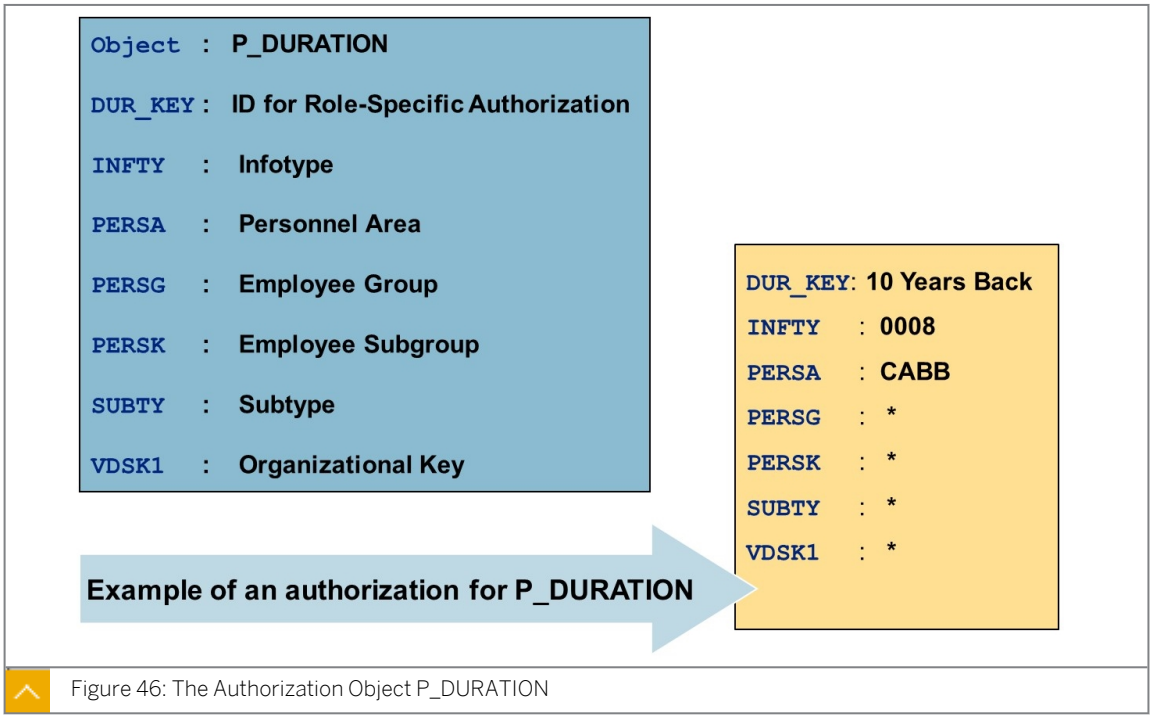

Figure 46: The Authorization Object P_DURATION

You can use the Authorization Periods for HR Master Data (P_DURATION) object in the authorization check for HR data. This check takes place when HR infotypes are being processed or read and is carried out as follows:

- When a user calls a report or a transaction to display or edit infotype data, the system checks whether the requested personnel data is authorized based on the organizational assignment of the user.

- If this is the case, the system checks whether the access authorization for the requested personal data at the infotype or subtype level is restricted by an authorization period in months. To do this, the system reads the settings in the Customizing activity *Define default authorization periods for infotypes and subtypes*.
- If a default authorization period is defined, the system checks whether this access authorization has been extended for specific roles (ID for role-specific authorization periods). To do this, the system reads the settings in the Customizing activity *Assign role-specific authorization periods to time period ID*.

The authorization object comprises the following fields:

- Data to which the user has access:
  - **INFTY** infotype
  - **SUBTY** subtype
- Organizational attributes of the clerk responsible (from infotype 0001, Organizational Assignment)
  - **PERSA** personnel area
  - **PERSG** Employee group
  - **PERSK** Employee subgroup
  - **VDSK1** organizational key
- Authorization period
  - **DUR_KEY ID** role-specific authorization periods

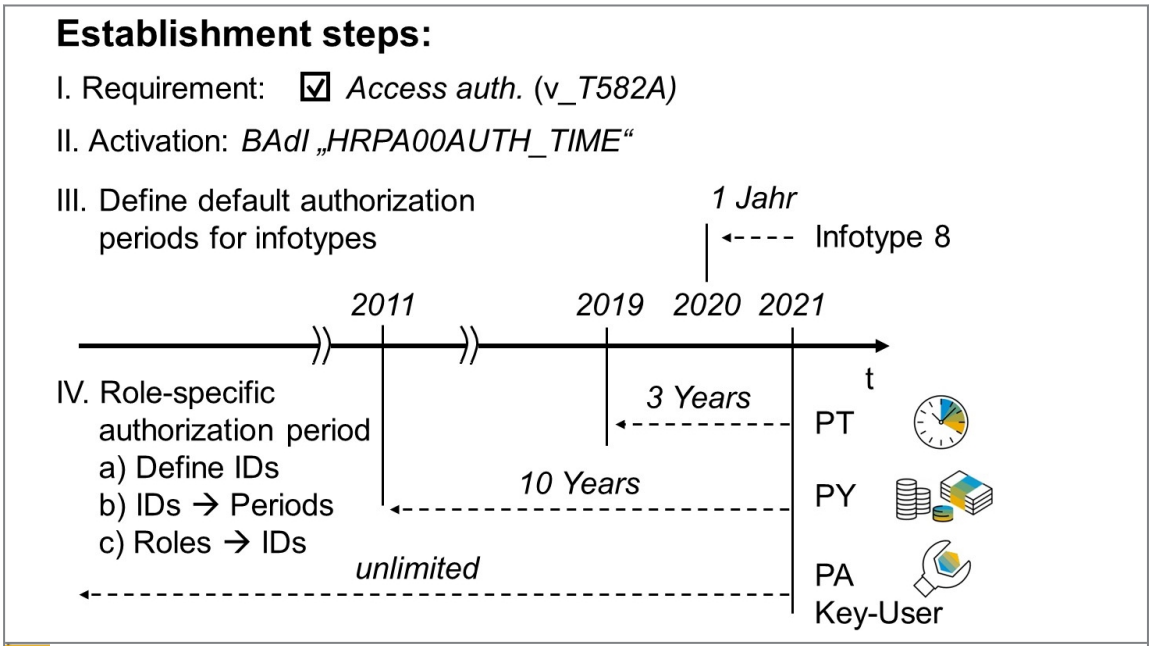

Figure 47: Time-Dependent Blocking of Data - Overview

To use all the options of the Time-Dependent Blocking of Data function, you must perform the following four steps in the SAP system:

I. Requirement: Set the Access auth. In the table v_T582A

If you want to limit the time of infotypes for display, you have to make a basic setting for this in the basic customizing of the infotypes. To do this, go to the customizing table v_T582A, select the infotype and mark the data field Access auth.

II. Activation : BAdI „HRPA00AUTH_TIME"

To activate the function of time-dependent blocking of data in principle, you have to implement and activate BAdI HRPA00AUTH_TIME.

III. Define default authorization periods for infotypes

In the past, you can restrict the display and maintenance of individual infotypes for all users.

IV. Role-specific authorization period

You can restrict the display and maintenance of infotypes from step III. Override this by creating a role-specific authorization period ID and assigning it to a new time period. You use this ID of a role in connection with the authorization object P_DURATION (Authorization Periods for HR Master Data). You assign this role to a user who usually has more extensive maintenance and display of infotypes in the past.

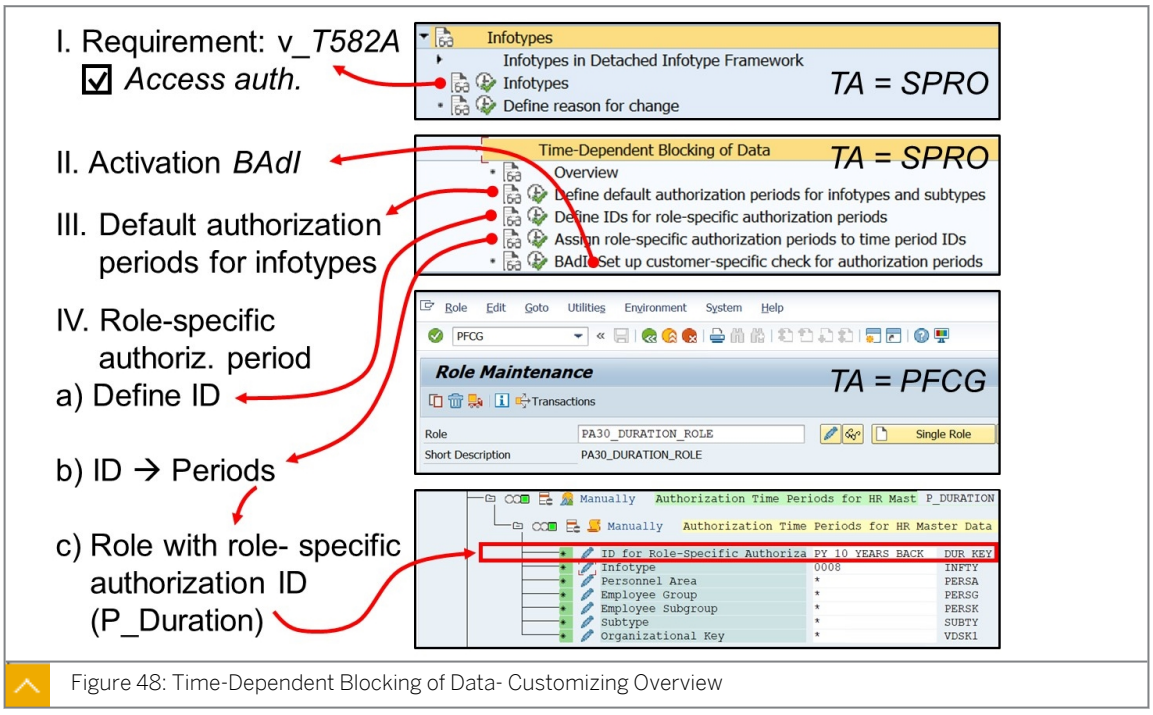

Figure 48: Time-Dependent Blocking of Data- Customizing Overview

To use all the options of the Time-Dependent Blocking of Data function, you must perform the four steps in the SAP system, as shown in the previous figure. In the current figure you can see a customizing overview for the implementation of this sequence.

For the step **I. Requirement: v_T582A** (Access auth.) go to customizing using the Transaction `SPRO` and use the following path *Personnel Management → Personnel Administration → Customizing Procedures → Infotypes*. Choose the IMG activity *Infotypes*. Alternatively, you can get to the customizing table using transaction `SM30` and table *v_T582A*.

For the steps

- II. Activation BAdI,
- III. Default authorization periods for infotypes and
- IV. Role-specific authorization period

go to customizing using the Transaction *SPRO* and use the following path *Personnel Management → Personnel Administration → Tools → Data Privacy → Block → Time-Dependent Blocking of Data.*

Finally, use the Role Maintenance (transaction `PFCG`) to use and set the role-specific authorization period ID.

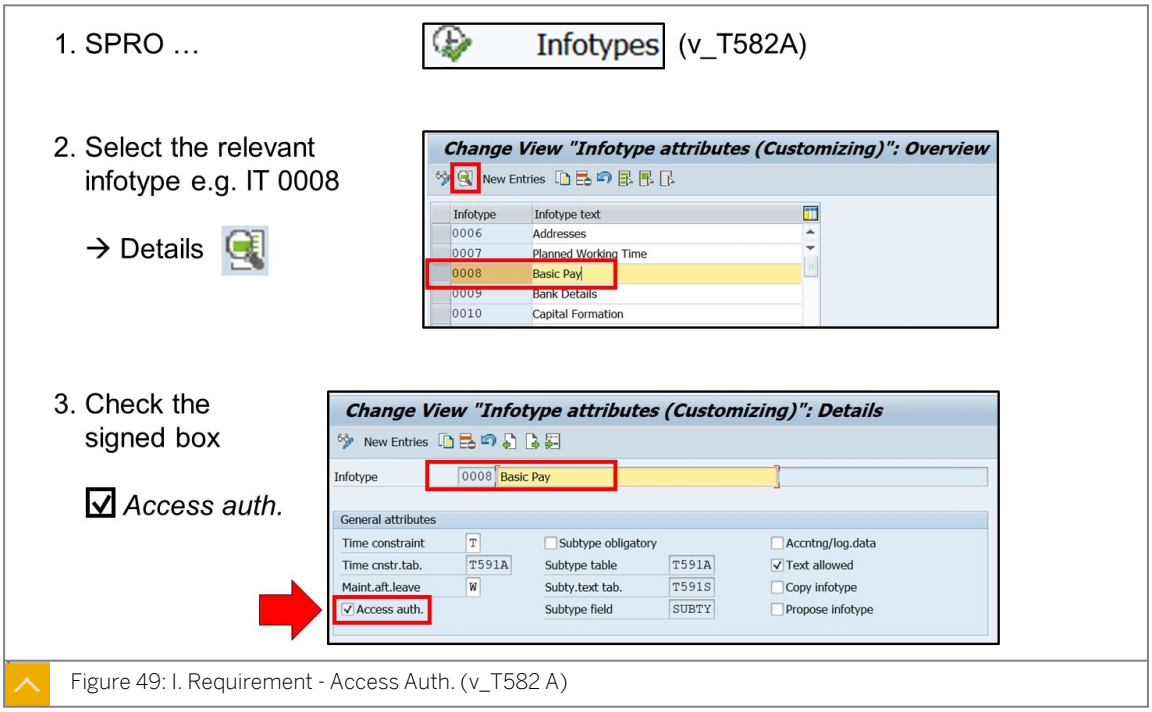

Figure 49: I. Requirement - Access Auth. (v_T582 A)

To use the *Time-Dependent Blocking of Data* function, you must set the *Indicator for access authorization* for each infotype.

If you want to check or set the indicator, you have to do the following:

1. Go to customizing using the Transaction `SPRO` and use the following path: *Personnel Management → Personnel Administration → Customizing Procedures → Infotypes*. Choose the IMG activity *Infotypes*. Alternatively, you can get to the customizing table using transaction `SM30` and table *v_T582A*.

2. In the screen Change view *Infotype attributes (Customizing)*: Overview, select the relevant infotype and click the *Details* button.

3. Check and select the check box *Access auth.* to activate the possibilities of the time-dependent blocking of data.

Details to the topic Indicator for access authorization

The Access auth. (access authorization) allows you to define the time period during which an HR-infotype can be accessed.When you access infotype data for a particular person (employee or applicant), the system reads his/her organizational assignment and the work area (infotype, subtype and authorization level). Each infotype will generally have records with different validity periods. One person may also have different organizational assignments (Organizational Assignment infotype (0001)) over a certain time period. If different administrators (users) are responsible for these organizational assignments, this is taken into account when the authorization for a specific infotype validity period is checked.

If you do not set this indicator (initial value), the administrator is authorized to access the infotypes if the person had, has or will have an organizational assignment which, in accordance with the authorization profile allows him/her to access this data.

If you set this indicator (X), the authorization check depends on the current (system) date.

II. BAdI activation

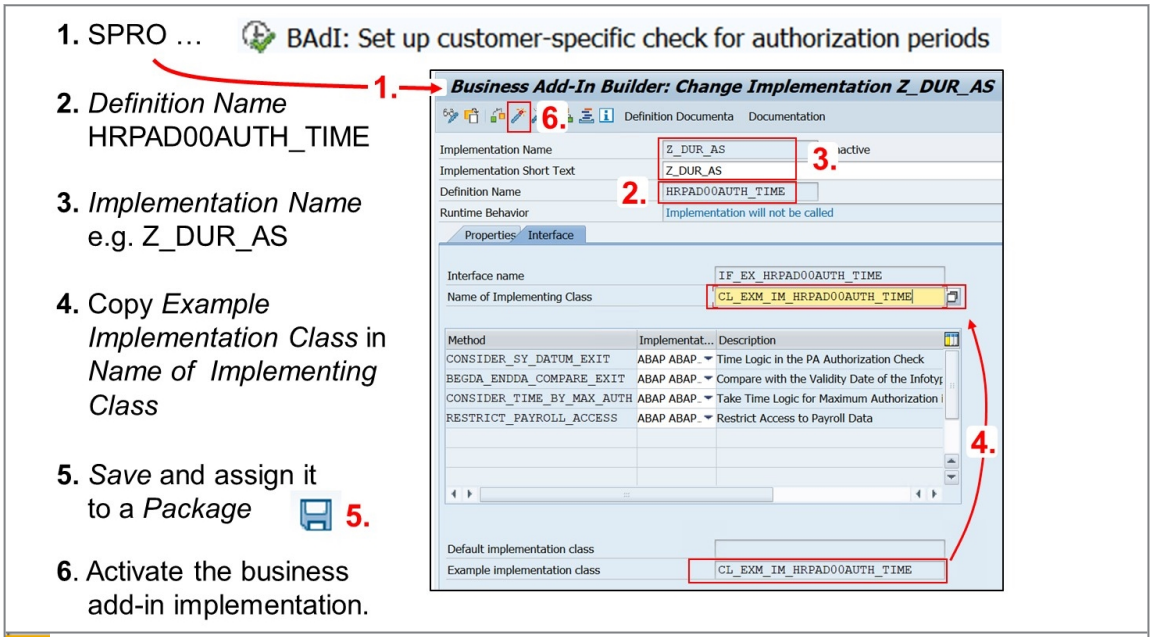

Figure 50: II. Activation of the BAdI HRPA00AUTH_TIME

With this Business Add-In (BAdI) *HRPA00AUTH_TIME* you can implement customer-specific time logic in the PA authorization check, thereby enhancing the standard SAP authorization check. To activate the BAdI, you have to do the following:

1. Go to customizing using the Transaction `SPRO` and use the following path *Personnel Management → Personnel Administration → Tools → Data Privacy → Block → Time-Dependent Blocking of Data*. Choose the IMG activity *BAdI: Set up customer-specific check for authorization periods*.
2. The Definition Name of the BAdI is *HRPAD00AUTH_TIME*.
3. Choose an Implementation Name like **`Z_DUR_AS`**.
4. Copy the ABAP class *CL_EXM_IM_HRPAD00AUTH_TIME* from the data field *Example Implementation Class* into the data field Name of Implementing Class.
5. Save the result and assign it to a package.
6. Activate the Business Add-In implementation.

Details and standard settings

This BAdI is not implemented in the SAP standard delivery (sample implementation). As long as you do not create a BAdI implementation, the system performs the standard authorization checks for HR master data without additionally restricting the time logic.

The BAdI includes the following methods:

- CONSIDER_SY_DATUM_EXIT

- BEGDA_ENDDA_COMPAR_EXIT
- CONSIDER_TIME_BY_MAX_AUTH
- RESTRICT_PAYROLL_ACCESS

For more information about the standard settings (filters, single or multiple uses), see the Properties tab in the BAdI Builder (transaction `SE18`).

III. Setting default authorization periods for Infotypes and Subtypes

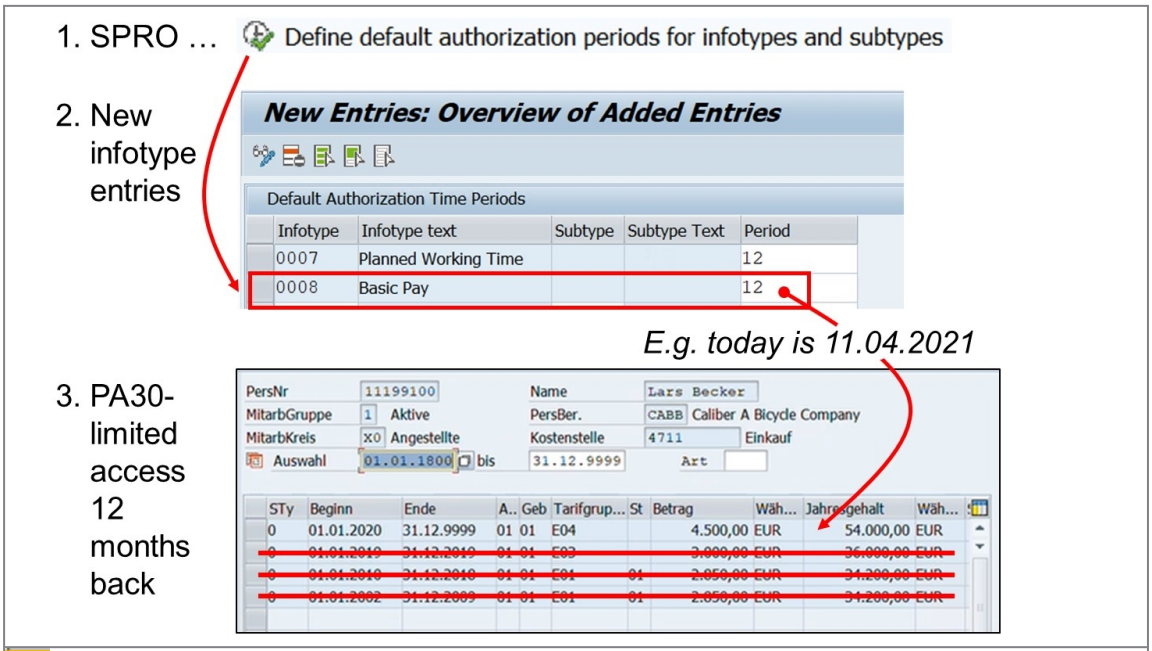

Figure 51: III. Default Authorization Periods for Infotypes and Subtypes

If you want to restrict access to the personal data, which is stored in infotypes and subtypes, the following things must be done:

1. Go to customizing using the Transaction `SPRO` and use the following path *Personnel Management → Personnel Administration → Tools → Data Privacy → Block → Time-Dependent Blocking of Data*. Choose the IMG activity *Define default authorization periods for infotypes and subtypes*.

2. Select the *Entries* button and enter an infotype/subtype with an assigned time period in months.

3. Test the access in the master data maintenance, for example using transaction `PA30`.

Details to the customizing "Define default authorization periods for infotypes and subtypes"

Use

In this Customizing activity you can define the minimum default authorization period with which you can restrict access to the personal data in the past, which is stored in infotypes and subtypes.

Depending on the country grouping, you specify a value (maximum of 30 characters) for the Authorization Period in Month for each infotype and subtype for all users, regardless of their roles.

Standard settings

The table is delivered empty. This means that access authorization for infotype and subtype data is not restricted. The time-dependent locking of data is not performed.

Activities

Check which minimum authorization periods for HR master data are required for all users in your country grouping and define the default authorization periods for each infotype and subtype. No entry means that the access authorization is not restricted.

IV. Setting role-specific authorization periods

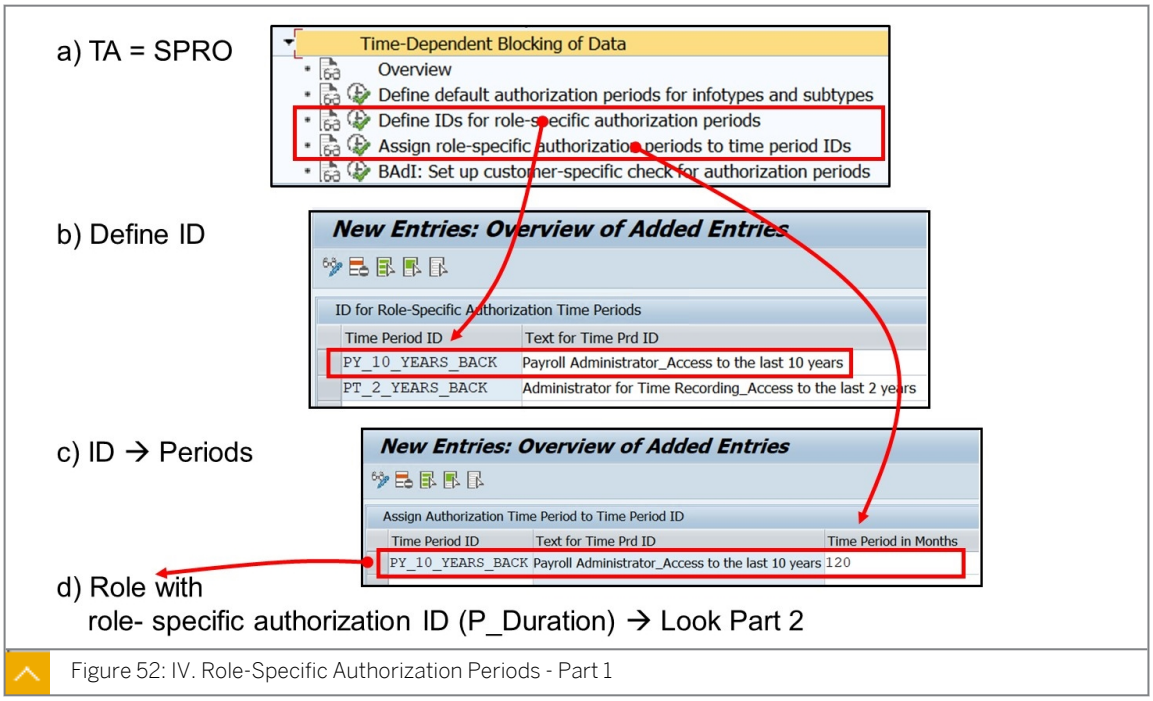

Figure 52: IV. Role-Specific Authorization Periods - Part 1

If you need different roles for different authorization periods in your company, this is where **you can define a time period ID** to identify these authorization periods (letter code with a maximum of 32 letters). In the Customizing activity *Assign Role-Specific Authorization Periods to Time Period IDs*, you create a country-specific Authorization Period in Months (30 characters maximum) for each Time Period ID.

You use the time period ID in the authorization object Authorization Time Periods for HR Master Data (P_DURATION). Based on the time period ID, you can enhance the default authorization period for displaying and editing HR data in the past, depending on the user roles.

To define IDs for role-specific authorization periods, you have to do the following steps:

a. Go to customizing using the Transaction `SPRO` and use the following path *Personnel Management → Personnel Administration → Tools → Data Privacy → Block → Time-Dependent Blocking of Data*. Choose the IMG activity *Define IDs for role-specific authorization periods*.

b. Choose the *New Entries* button and set a Name for the Time Period ID, for example **`PY_10_YEARS_BACK`**.

c. Go to customizing using the Transaction `SPRO` and use the following path *Personnel Management → Personnel Administration → Tools → Data Privacy → Block → Time-Dependent Blocking of Data*. Choose the IMG activity *Assign Role-Specific Authorization*

Periods to Time Period IDs. Set the *Time Period ID* for example **PY_10_YEARS_BACK** and assign a *Time Period in Months* -for example- **120**.

Activities and Examples

Check which roles in your company need specific authorization periods and create the necessary time period IDs with the related texts.

For example, HR administrators, payroll administrators, and power users all need different authorization periods. The relevant entries in the Customizing views look like this:

Table 7: Entries per user group

Time Period ID	Time Period ID Text
HR_ADMIN	HR Administrator
PAYROLL_ADMIN	Payroll Administrator
POWER_ADMIN	Power User

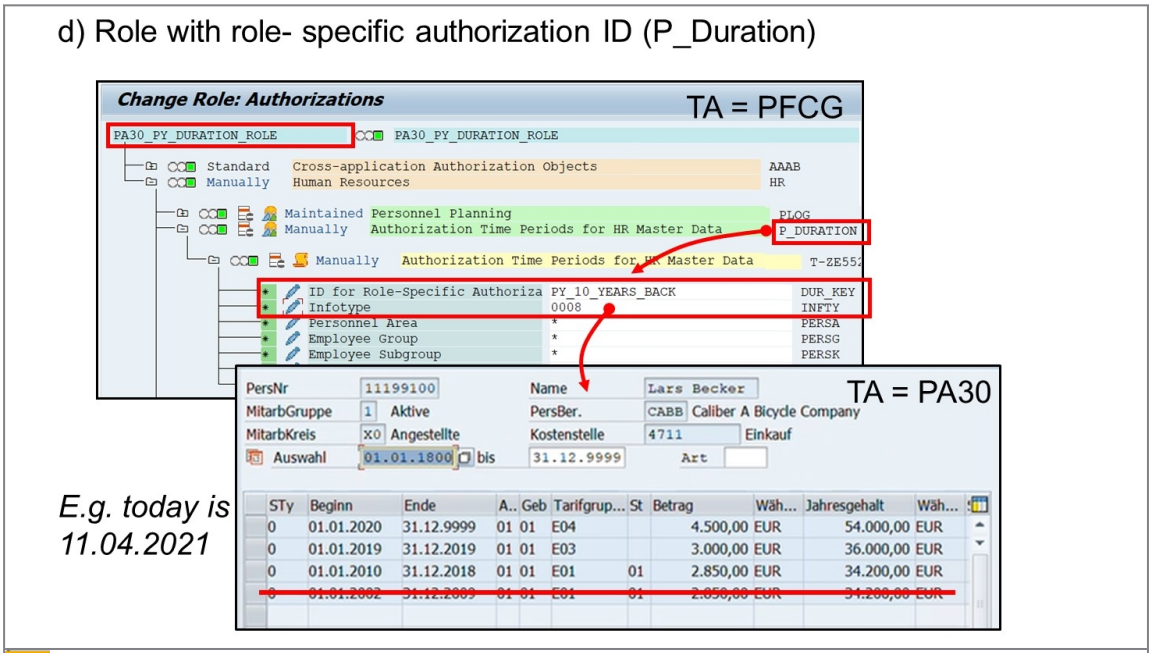

Figure 53: IV. Role-Specific Authorization Periods - Part 2

d) Maintenance of the user roles:

Edit the authorizations and use the time period ID to assign the user role a role-specific authorization period. Use the authorization object *P_DURATION* ("Authorization Periods for HR Master Data") for this.

Example

The figure shows a role with the authorization object *P_DURATION* as an example. The authorization field *ID for Role-Specific Authorization* is assigned the ID **PY_10_YEARS_BACK**. The *Infotype authorization* field is assigned to **0008** (Basic Pay). If you assign a user this role, he or she will be able to access data records of infotype **0008** (Basic Pay) ten years in the past.

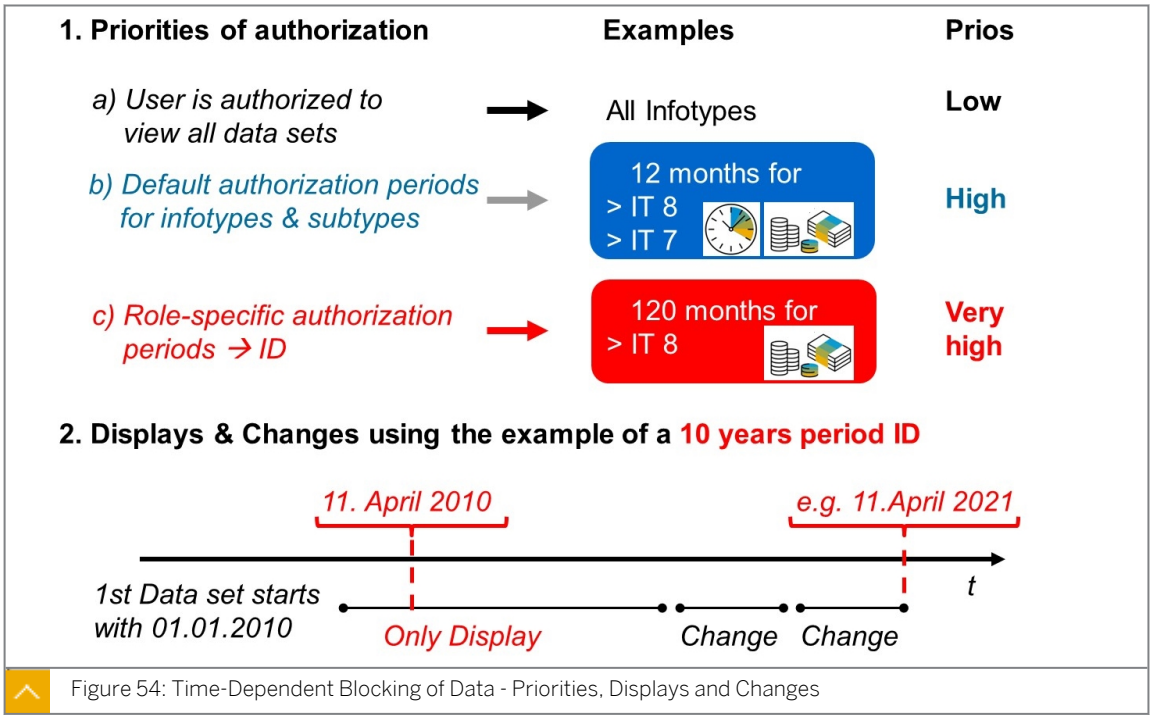

Figure 54: Time-Dependent Blocking of Data - Priorities, Displays and Changes

1. Priorities of authorization

When setting up HCM authorizations for reading and editing employee data records, there are many different options for customizing settings. In some cases, different customizing settings compete with one another. In this case there is a sequence of priorities, i.e. a sequence of which settings are more highly weighted. This sequence of priorities is as follows:

a) Low Priority: User is authorized to view all data sets.

b) High Priority: Default authorization periods for *infotypes & subtypes*.

c) Very High Priority: Role-specific authorization periods IDs.

2. Displays & Changes

When using the customizing Time-Dependent Blocking of Data, only data records can be **read and changed** whose start date is within the authorization period. If only the end date is within the authorized period, the data record can at least be read.

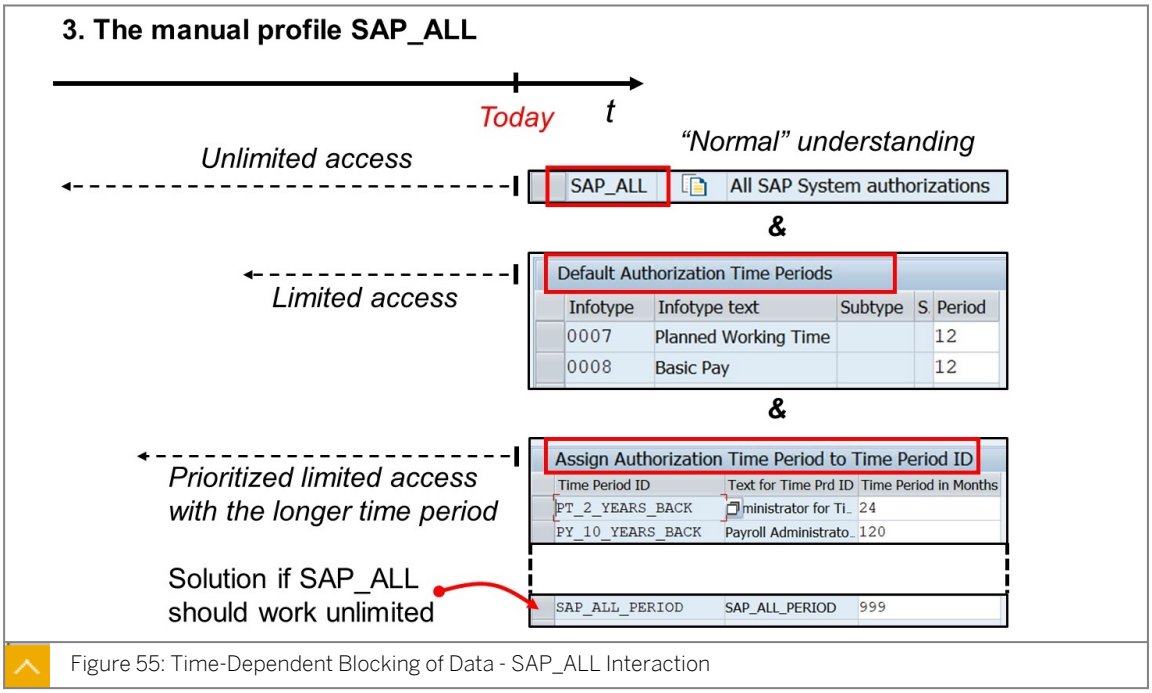

Figure 55: Time-Dependent Blocking of Data - SAP_ALL Interaction

3. The manual profile SAP_ALL

If you assign the manual profile SAP_ALL to a user, the user has all authorizations in the current SAP system. The assumption sounds logical for two reasons:1. Authorizations in AS-ABAP are always additive. This means that once assigned authorizations can only be supplemented, but usually not restricted.

2. The name of the manual profile SAP_ALL suggests that you have full authorization for this SAP system.

However, both assumptions do not apply in connection with HCM in general and for the topic of Time-Dependent Blocking of Data in particular.

The SAP HCM module has such special requirements that exclusion and restrictions are not unusual. This applies, for example, to the restrictions imposed by the authorization object *PERNR*, the structural authorizations and also to the topic of *Time-Dependent Blocking of Data.*

Even when assigning the manual profile *SAP_ALL*, you cannot rely on having all authorizations in the SAP system. In principle, the *SAP_ALL* calculations are restricted by the customizing *Time-Dependent Blocking of Data*.

Specifically, the following applies:

1. Customizing *Default Authorization Time Periods* restricts the *SAP_ALL* authorization for maintaining and displaying infotypes. This means that you only have limited access to data records in the past.

2. The Customizing *Assign Authorization Time Period ID* prioritizes the *SAP_ALL* authorization for maintaining and displaying infotypes in the past. The users do not have to be assigned a role with the corresponding *Time Period ID (P_DURATION)*. One entry in the table is sufficient. If there are several entries, the restriction applies with the longer time period.

Note:
If you want to maintain unlimited access to data records in the past using the manual profile *SAP_ALL*, enter an entry with the *Time Period in Months* of **999** in the *Assign Authorization Time Period ID* table.

LESSON SUMMARY
You should now be able to:

- Outline read access time logic
- Outline write access time logic
- Describe the application of time-dependent logic
- Lock the data using the time-dependent authorization

Learning Assessment

1. What infotype is read to determine the period of responsibility?

2. What infotype is read to determine the period of responsibility?

3. What infotype is read to determine the period of responsibility?

4. What factors are processed by the time logic for master data access?

   Choose the correct answers.

   - ☐ A The user's period of responsibility.
   - ☐ B The time of access.
   - ☐ C The access type (read or write).
   - ☐ D The validity area of the infotype.

Learning Assessment - Answers

1. What infotype is read to determine the period of responsibility?

   The Organizational Assignment infotype.

2. What infotype is read to determine the period of responsibility?

   The Organizational Assignment infotype.

3. What infotype is read to determine the period of responsibility?

   The Organizational Assignment infotype.

4. What factors are processed by the time logic for master data access?

   Choose the correct answers.

   - [X] A The user's period of responsibility.
   - [ ] B The time of access.
   - [X] C The access type (read or write).
   - [X] D The validity area of the infotype.

   Correct. The time logic processes the user's period of responsibility, access type, and validity area of infotype.

UNIT 5 Payroll Authorization Objects

UNIT OBJECTIVES

- Outline authorizations used for the personnel control record
- Outline authorizations used to control the posting of payroll results to accounting
- Outline the authorizations used for the off-cycle workbench
- Set up an authorization to control access to schemas and personnel calculation rules

Unit 5
Lesson 1

Defining Payroll Authorization Objects

LESSON OVERVIEW
This lesson outlines the authorization objects for the personnel control record, posting to accounting, and the off-cycle workbench.

Business Example:

As a member of the authorizations team, you are responsible for the maintenance of authorizations for various aspects of the payroll process. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline authorizations used for the personnel control record
- Outline authorizations used to control the posting of payroll results to accounting
- Outline the authorizations used for the off-cycle workbench

Authorization Object for the Personnel Control Record

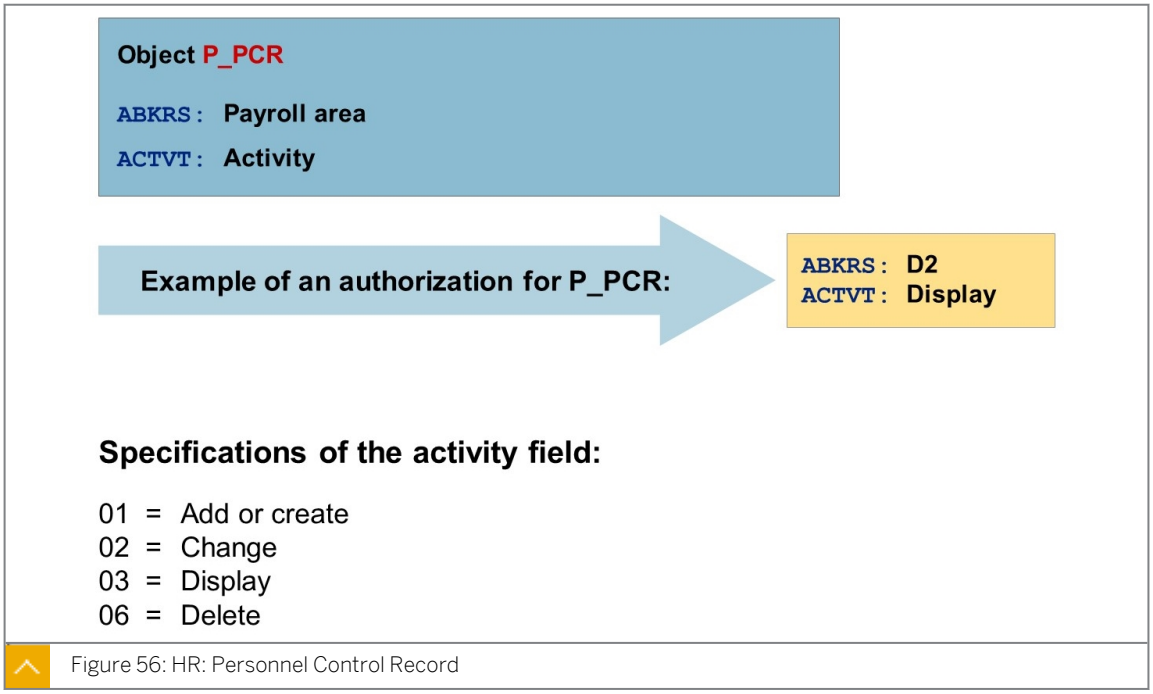

Figure 56: HR: Personnel Control Record

The personnel control record authorization object is used by the authorization check for the payroll control record. This check takes place when the control record is displayed using

transaction code PA03, or when the control record is maintained. The check also takes place in particular during maintenance using the payroll menu.

Payroll Posting to Accounting

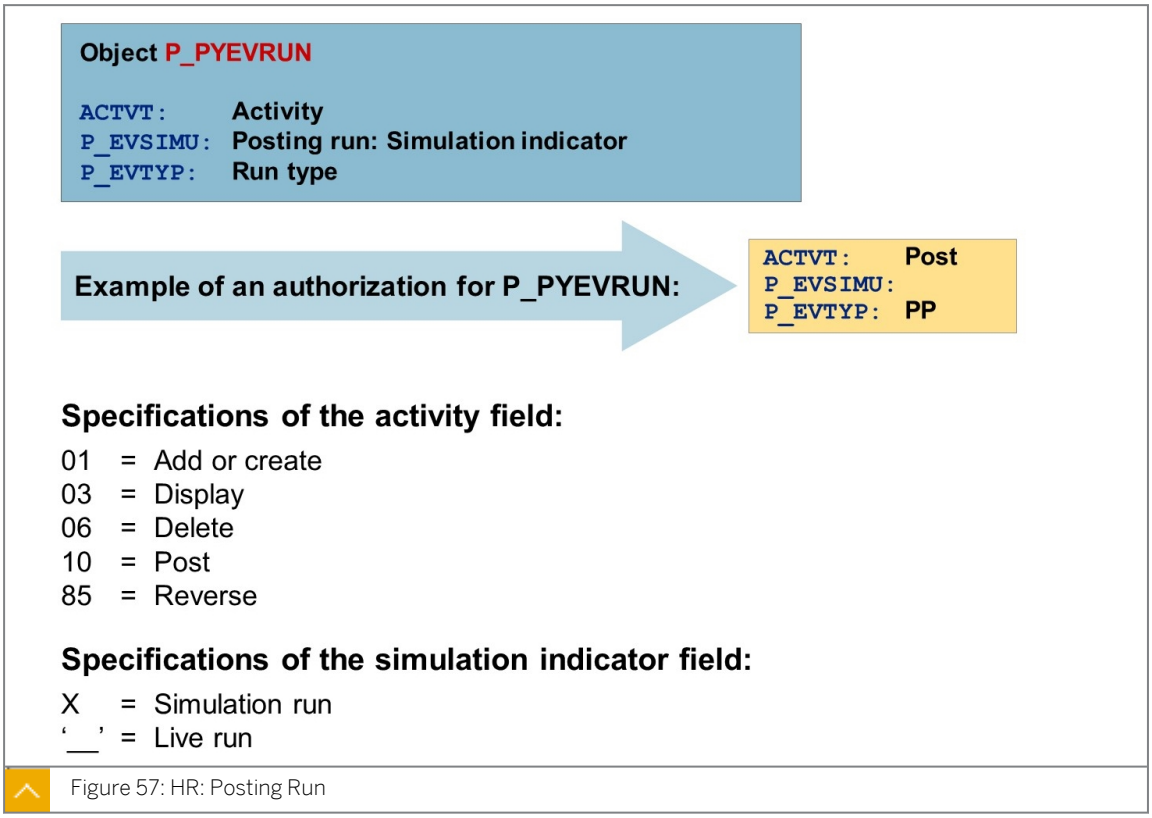

Figure 57: HR: Posting Run

You can use this authorization object to control the actions possible for posting runs.

The following entries are possible in the *run type* field:

- AP Posting tax or SI Austria
- PP Payroll posting
- TP Posting third-party remittance
- TR Travel expenses posting
- ZA Payroll evaluation in South Africa

HR: Posting Document

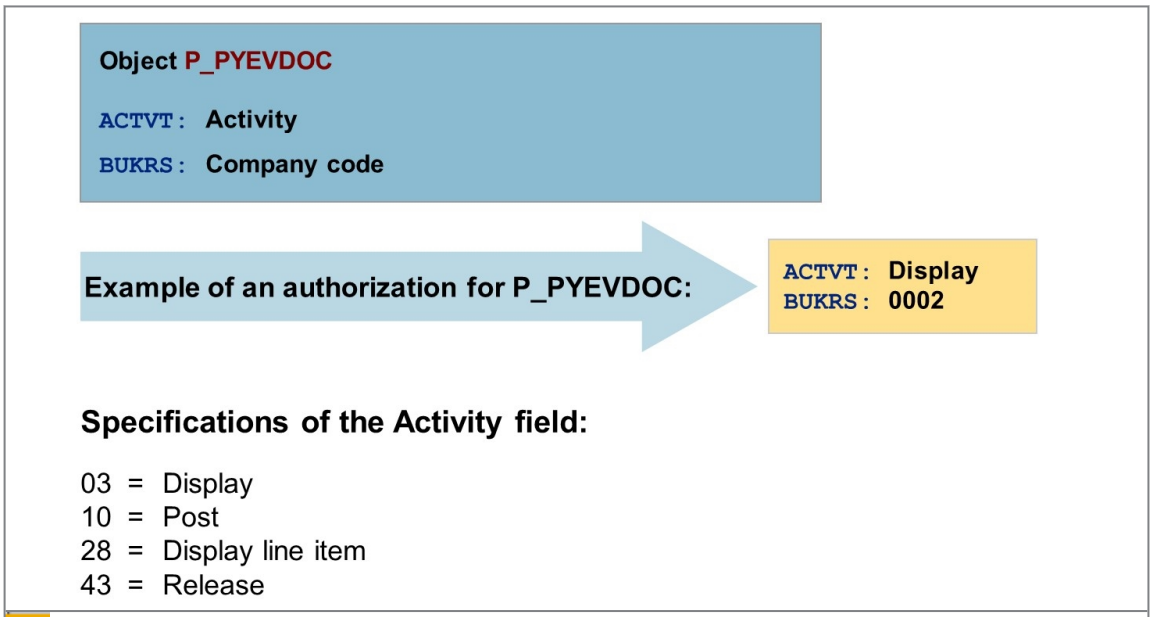

Figure 58: HR: Posting Document

You use this authorization object to protect actions on posting documents.

Authorization Object for the Off-Cycle Workbench

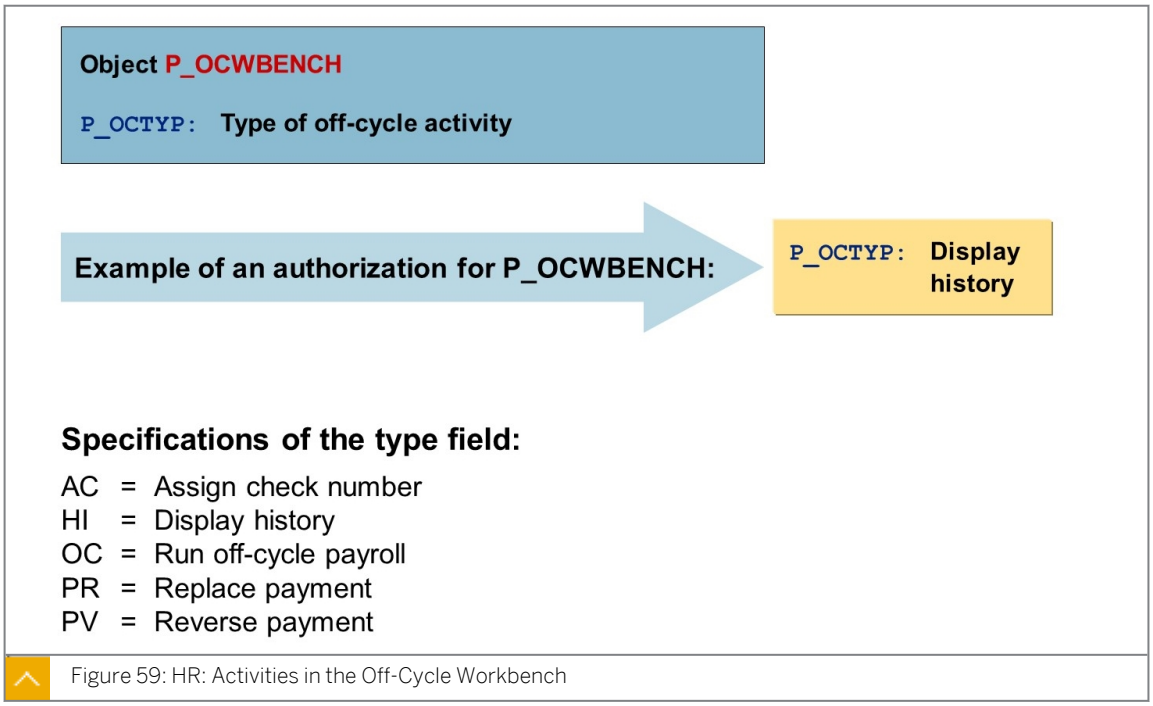

Figure 59: HR: Activities in the Off-Cycle Workbench

This authorization object is used during the authorization check for the off-cycle workbench. Each administrator sees only the off-cycle activities that he or she is authorized to perform.

LESSON SUMMARY

You should now be able to:

- Outline authorizations used for the personnel control record
- Outline authorizations used to control the posting of payroll results to accounting
- Outline the authorizations used for the off-cycle workbench

Controlling Access to Schemas and Personnel Calculation Rules

LESSON OVERVIEW
This lesson outlines the authorization objects used for schemas and personnel calculation rules.

Business Example:

As a member of the authorizations team, you are responsible for setting up authorizations to control access to schemas and personnel calculation rules. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Set up an authorization to control access to schemas and personnel calculation rules

Authorization Object for Schemas and Personnel Calculation Rules

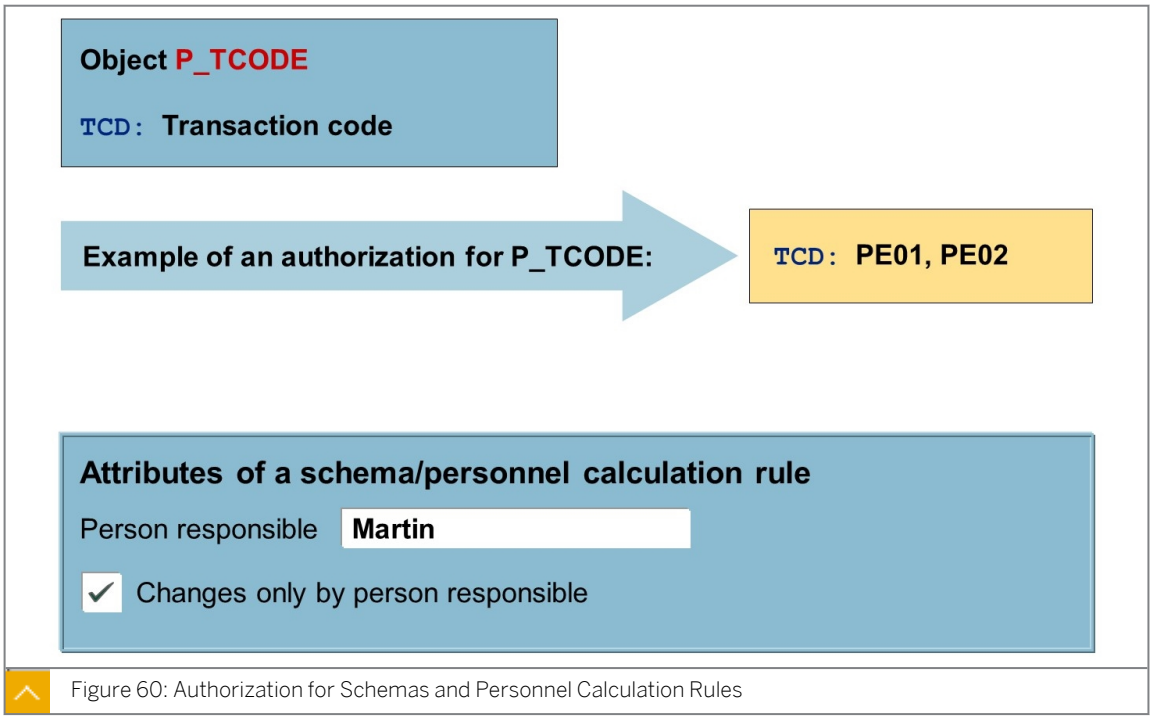

Figure 60: Authorization for Schemas and Personnel Calculation Rules

Access authorization to payroll schemas (transaction **PE01**) and personnel calculation rules (transaction **PE02**) is granted by an authorization for the *HR: Transaction Code*.

If change authorization should only be granted to the employee specified as the person responsible in the attributes of the schema or rule, you must activate the field *Changes Only*

by Person Responsible in the attributes. If this indicator is set, other employees are granted only **read authorization** for the schema or rule.

This attribute can only be removed by the employee responsible or by running the **RPUCTF00** report, *Change Attributes for Schemas and Personnel Calculation Rules*.

Hint:
The authorization objects *HR: Authorization for Personnel Calculation Schemas* and *HR: Authorization for Personnel Calculation Rules* contained in the HR object class are not used in the standard system.

LESSON SUMMARY
You should now be able to:

- Set up an authorization to control access to schemas and personnel calculation rules

Learning Assessment

1. What are the authorization objects for the payroll posting run?

2. How can you ensure that only the person authorized may change a schema or personnel calculation rule?

Learning Assessment - Answers

1. What are the authorization objects for the payroll posting run?

   HR: Posting run and HR: Posting document

2. How can you ensure that only the person authorized may change a schema or personnel calculation rule?

   You can do so by setting a flag in the field *Changes Only by Person Responsible* in the attributes of the schema or personnel calculation rule.

UNIT 6 Authorization Check for Evaluations

UNIT OBJECTIVES

- Set up the selection period for an evaluation
- Determine if personnel numbers were skipped during authorization checks
- Create an authorization for the HR reporting object for payroll reports

Unit 6
Lesson 1

Setting Up Selection Periods for Evaluations

LESSON OVERVIEW
This lesson describes the person and data authorization check and shows you how to set up the selection period.

Business Example:

As a member of the authorizations team, you are responsible for setting up person and data authorization checks. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Set up the selection period for an evaluation
- Determine if personnel numbers were skipped during authorization checks

Person and Data Authorization Check

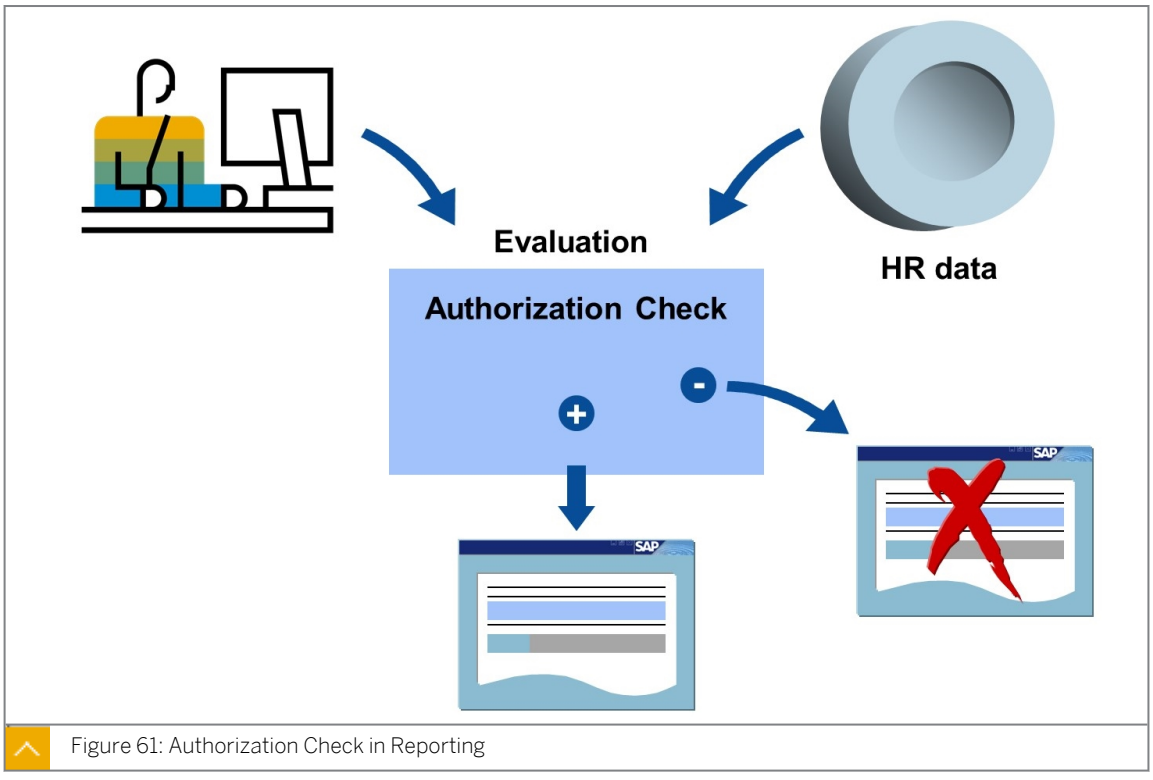

Figure 61: Authorization Check in Reporting

The HR logical databases are used in many reports and provide certain generic functions such as selection and the authorization check.

The authorization check establishes whether the user who starts the evaluation has the required authorizations for the data to be evaluated.

In reporting for HR master data, we distinguish between an authorization for persons and an authorization for data.

Authorization for Persons

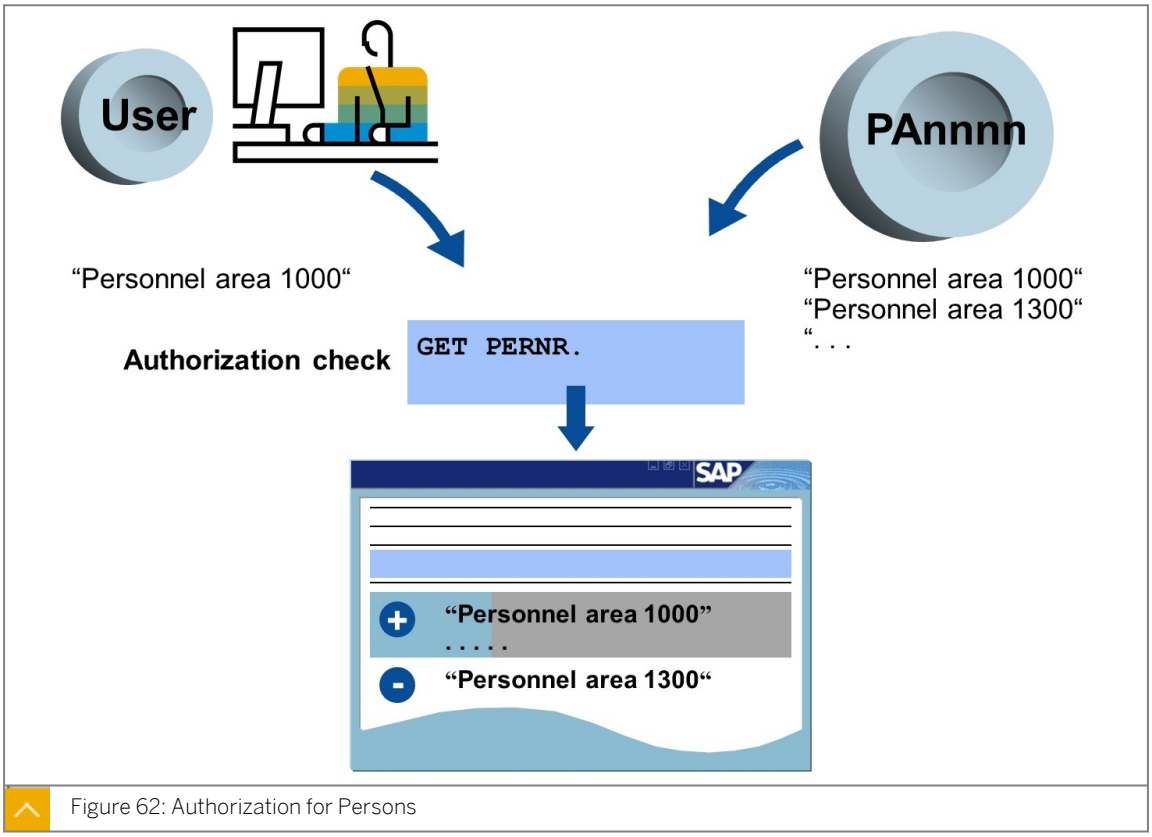

Figure 62: Authorization for Persons

Authorization for persons: At the GET PERNR point in the authorization check and for the set of selected employees, the system checks whether the user has authorization for the organizational features of the employee. In the figure Authorization for Persons, the administrator has authorization only for personnel area 1000.

During the evaluation, the system skips employees for whom no authorization exists. At the end of the evaluation, the number of employees skipped because of missing authorizations is returned.

Authorization for Data

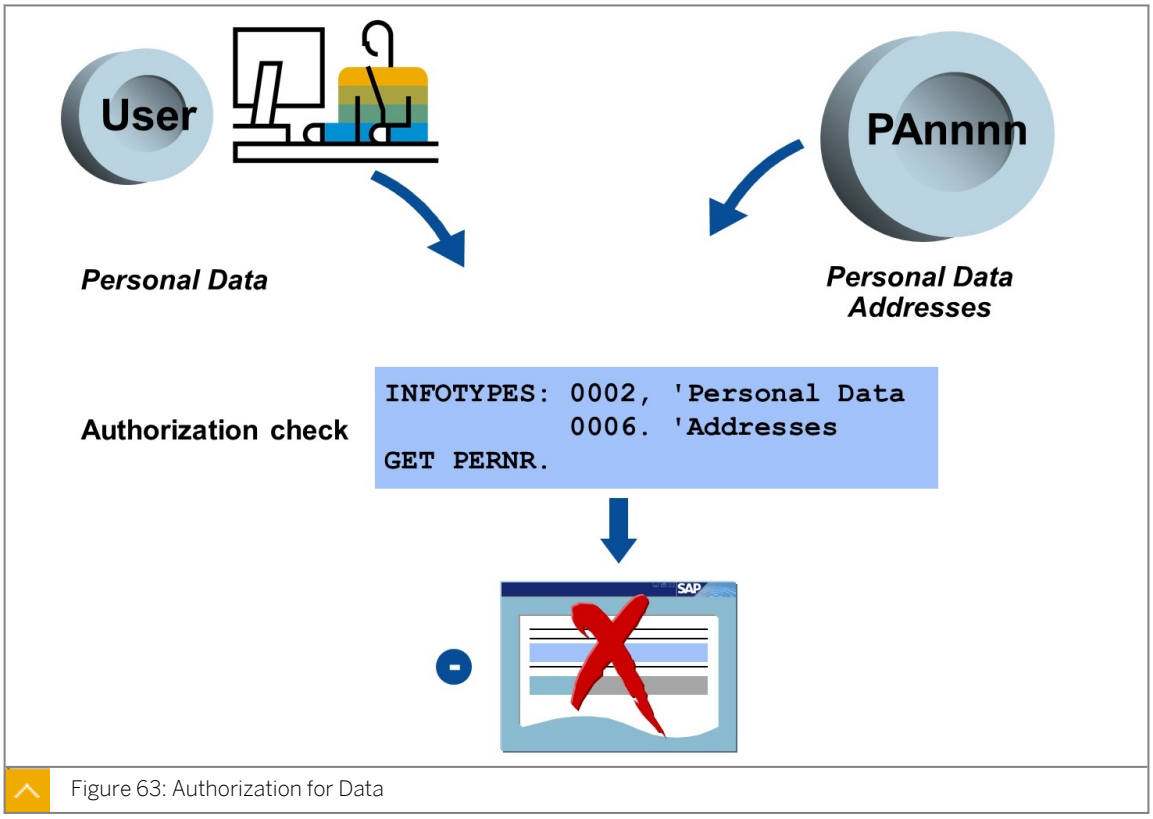

Figure 63: Authorization for Data

Authorization for data: The system checks whether the user has authorization for all the infotypes used in the evaluation.

In this example, the user has authorization for the *Personal Data* infotype (0002) but not for the *Addresses* infotype (0006).

If the user has no authorization for an infotype, the evaluation terminates with an error message.

Partial Authorization for Data

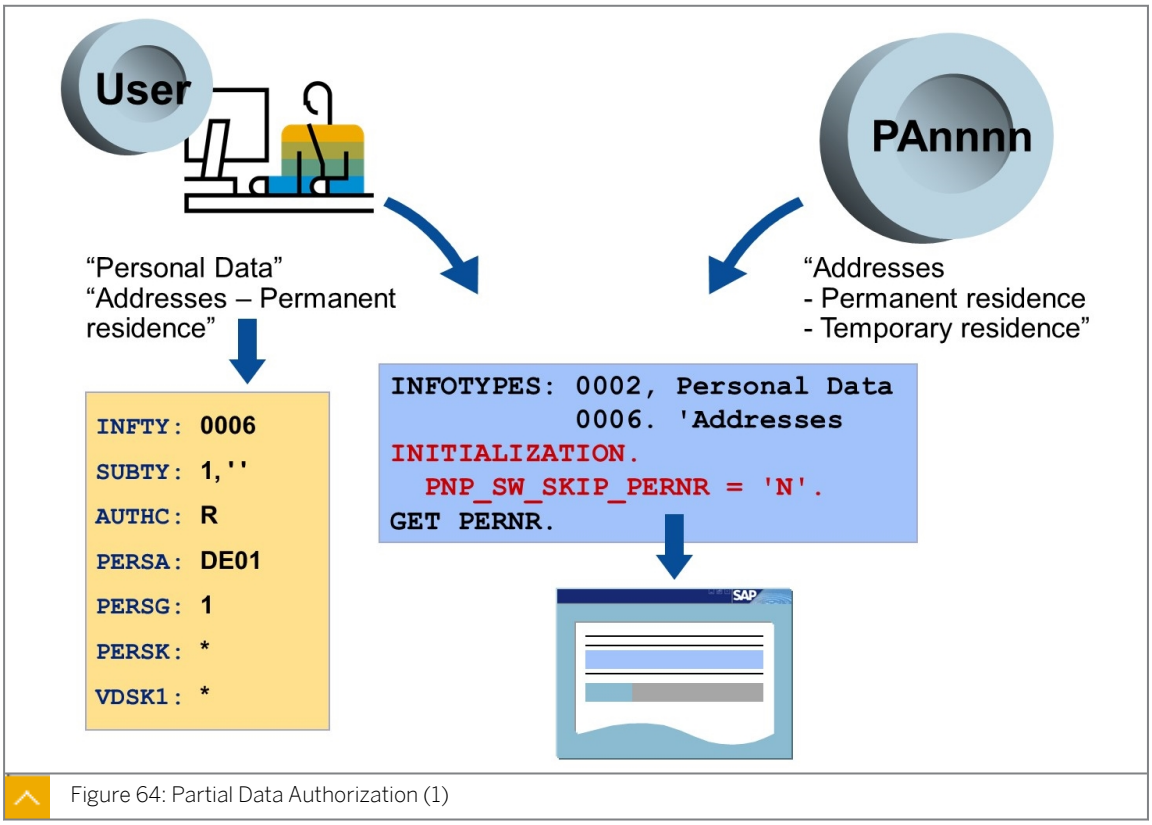

Figure 64: Partial Data Authorization (1)

In this example, the user has authorization for the *Personal Data* infotype (0002). For the *Addresses* infotype (0006), the user has authorization only for the *Permanent Residence* subtype (1) but not for the *Temporary Residence* subtype (2).

If there is no authorization for certain data selected on a personnel number (in the example, the personnel number that is read by the logical database has a record of infotype 0006, subtype 2), the logical databases cannot determine how best to respond to the special request. As long as nothing to the contrary is determined in the code, personnel numbers for which all data records except one can be accessed by users are completely skipped.

A report, such as the one in the example, that should output only address data can continue to run using partial data of a personnel number. In such a case, you can program the logical database not to skip personnel numbers. However, only the data for which authorizations exist is made available to the relevant reports. There is no direct way to access the data that was not read by the authorization check. The setting is made in the report at the INITIALIZATION time of processing by the PNP_SW_SKIP_PERNR = 'N' statement.

This option is available in the SAPDBPNP logical database only.

Partial Authorization for Data (2)

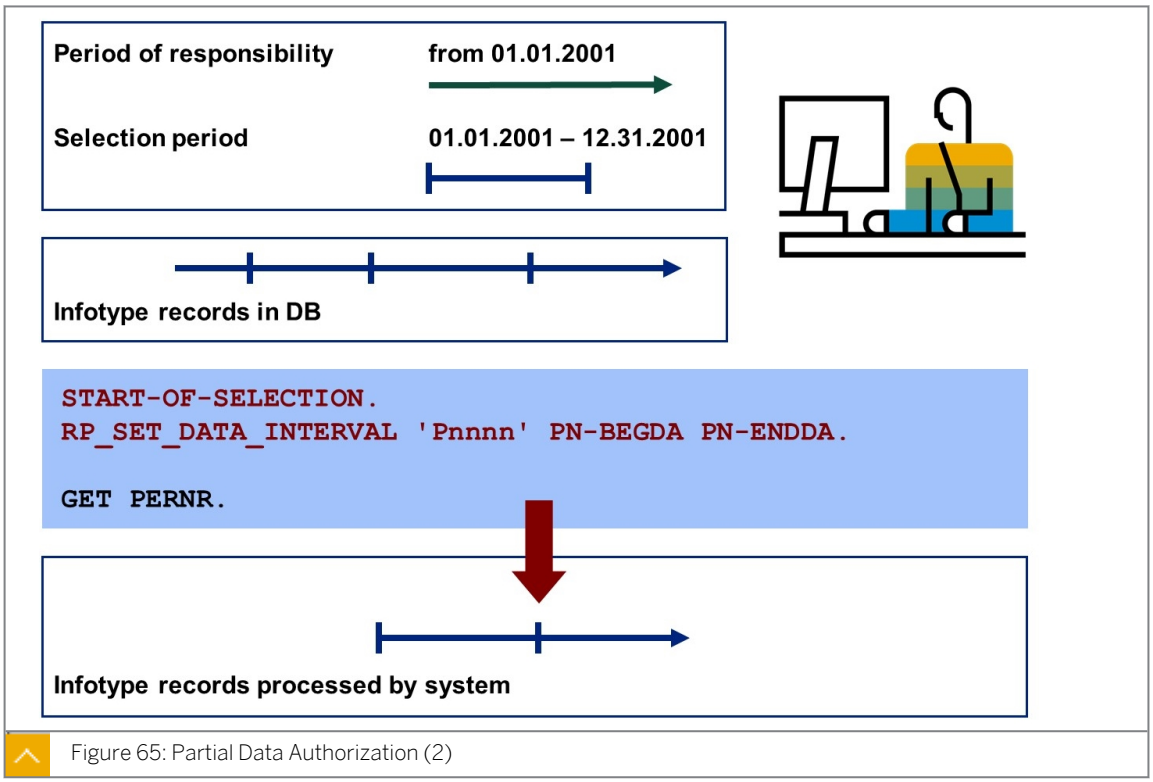

Figure 65: Partial Data Authorization (2)

A report that runs evaluations by personnel number generally works best if it can read all the data requested on the personnel number concerned.

However, the evaluation for a certain selection period may now be possible but not for a longer selection period. Normally, the logical database always selects all the data of an infotype and checks the authorization. If you want the system to read and check only the data of the selection period, you can use the RP_SET_DATA_INTERVAL macro (START-OF-SELECTION) for this.

LESSON SUMMARY

You should now be able to:

- Set up the selection period for an evaluation
- Determine if personnel numbers were skipped during authorization checks

Unit 6
Lesson 2

Creating Authorizations for the HR: Reporting Object

LESSON OVERVIEW
This lesson shows you how to create an authorization object to control access to payroll results.

Business Example:

As a member of the authorizations team, you are responsible for controlling access to payroll results and ensuring optimal system performance. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Create an authorization for the HR reporting object for payroll reports

HR Reporting Authorization Object

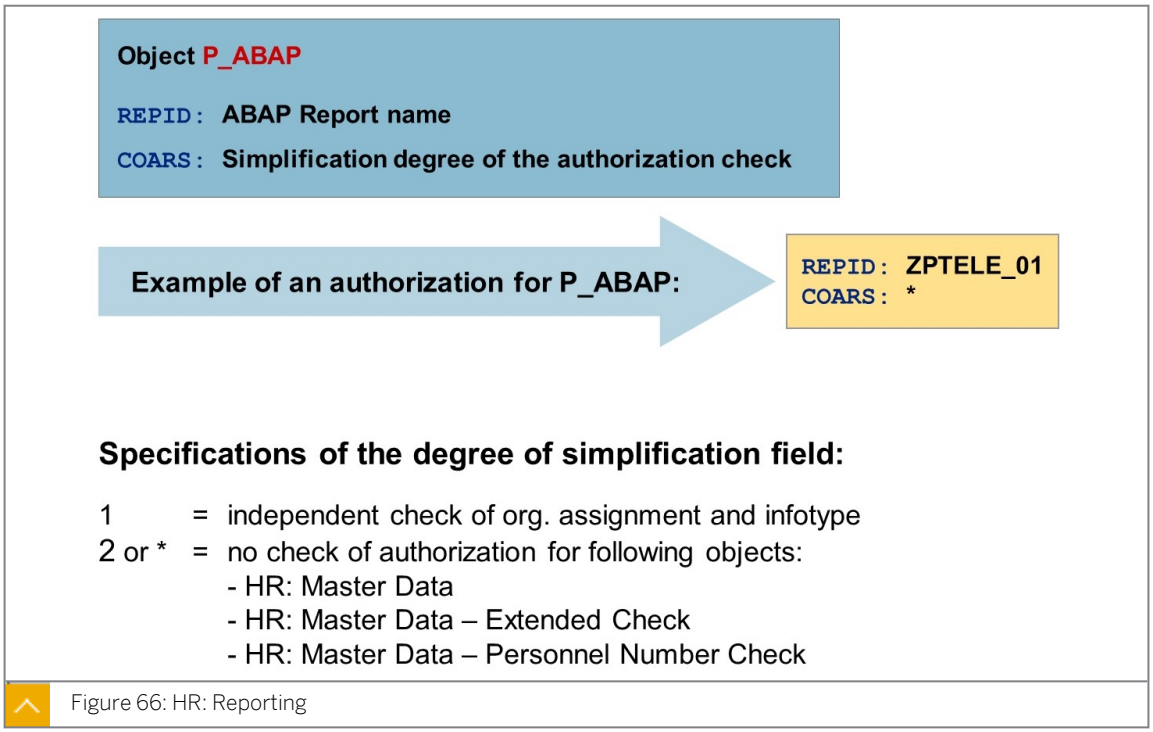

Figure 66: HR: Reporting

You can use relevant authorizations for this object to control how the objects P_ORGIN, P_ORGXX, and the customer-specific authorization object P_NNNNN are used in the specified reports to check the authorization for HR infotypes. You can also use reports to control the infotype authorization check. This can be useful for functional reasons or to

improve performance (for example, of the payroll run) at runtime of the corresponding reports.

For this object, enter one or more report names and a degree of simplification (COARS field) that the check is to use for the report(s) concerned.

If you regard certain HR reports (*telephone lists* and so on) as uncritical with relation to access protection, enter the corresponding reports in the *Report name* field and * in the *Degree of Simplification* field. Consequently, no other checks except for the check on the S_PROGRAM object, *ABAP: Program Flow Checks*, take place.

Hint:
A P_ABAP authorization, for example for report SAPDBPNP with COARS = 2, means that all HR reports based on the PNP logical database can perform no more authorization checks. You will want to deactivate the authorization checks for only a very small number of reports. In case of doubt, do not assign your users authorizations for the P_ABAP object.

HR: Reporting in Time Evaluation

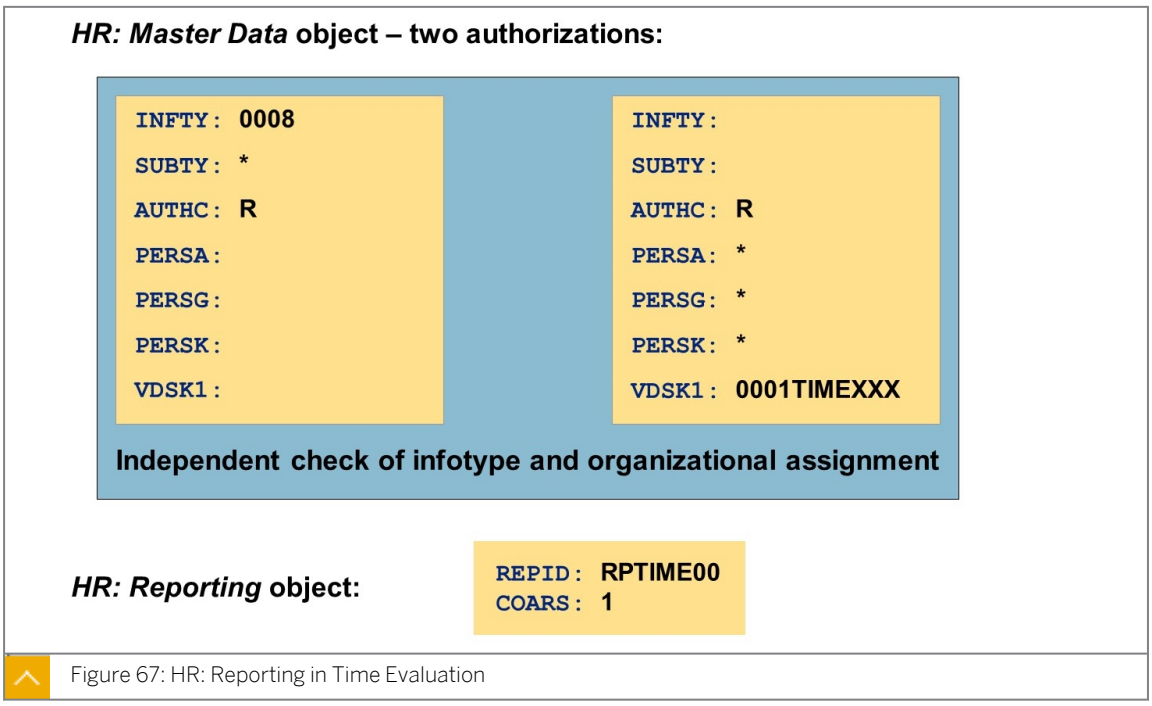

Figure 67: HR: Reporting in Time Evaluation

A time administrator should perform time evaluations (*Time Evaluation* report, RPTIME00) for employees assigned the organizational key CABB*. To obtain certain additional information that is required internally (information that the program user cannot see or can see only partially), the system must read the *Basic Pay* (0008) infotype, among others, during time evaluation. To be able to carry out time evaluation, the time administrator must have display authorization for this infotype. However, the administrator should not have general display authorization for the Basic Pay (0008) infotype. To restrict the read authorization for the *Basic Pay* (0008) infotype for employees with the CABB* organizational key in report RPTIME00, use the authorizations shown in the figure HR: Reporting in Time Evaluation.

As a result, a simplified check takes place in connection with report RPTIME00 during the infotype authorization check. On the one hand, infotype, subtype, and level are checked

independently according to simplification degree 1, and on the other hand, organizational assignment (in the example, *organizational key*). Infotype 0008 can be read in report RPTIME00. If, however, the check is not in connection with this report, all fields of the *HR: Master Data* object are checked together. This check does not result in read access to the *Basic Pay* infotype.

System Performance Improvement

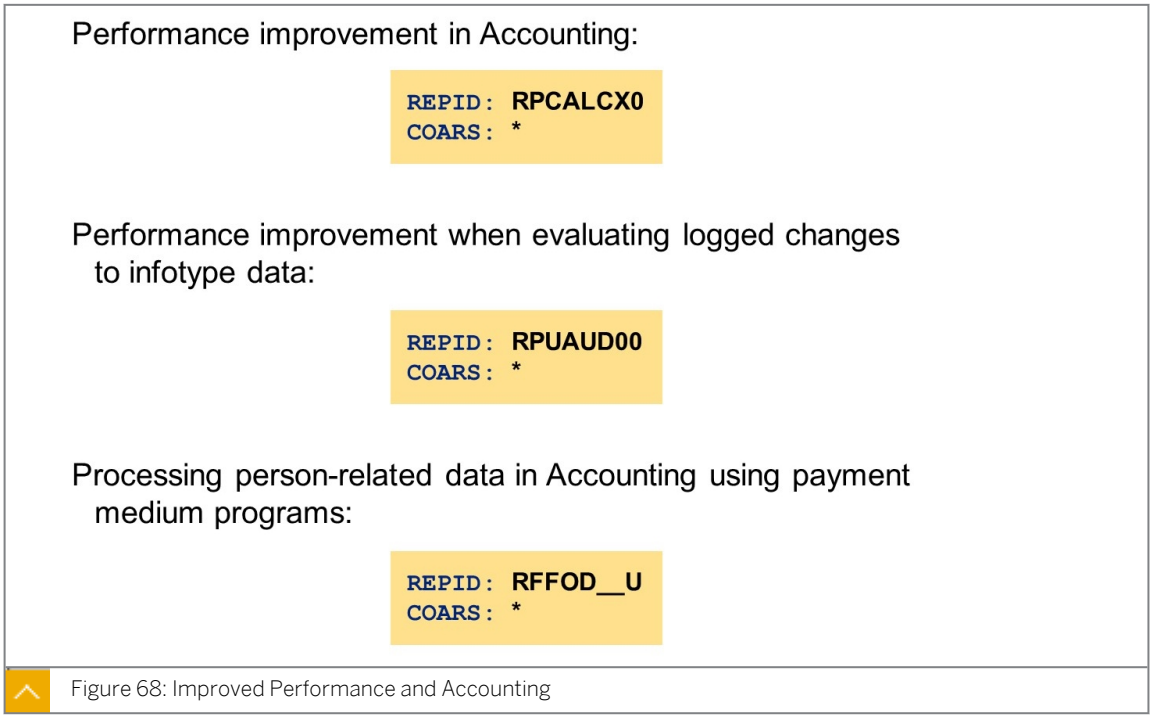

Figure 68: Improved Performance and Accounting

If the runtime of the payroll driver is very long due to the large number of personnel numbers to be processed, it makes sense to switch off the authorization check to improve performance.

Evaluations of the logged changes in infotype data are subject to infotype authorization checks. The person who starts this kind of evaluation normally has extensive infotype authorizations. In this case, it makes more sense to assign the user a global authorization using the RPUAUD00 report (*Logged Changes to Information Types Data*) rather than to check individual data. To do so, use an authorization for the existing object that has the value RPUAUD00 in the *Report name field (REPID) and the value 2 or * in the Degree of simplification field (COARS)*.

The payment medium programs in Accounting processes extremely sensitive person-related data. As an additional security measure, the system checks whether the user has corresponding authorization for the existing object and checks whether the user is authorized to start the program. You must enter the name of the payment medium program in the *Report name* field and the value 2 or * in the *Degree of simplification field*.

LESSON SUMMARY

You should now be able to:

- Create an authorization for the HR reporting object for payroll reports

Learning Assessment

1. Does reporting in HR require additional authorizations?

2. What program names may not be entered in the authorization for object HR: Reporting?

Learning Assessment - Answers

1. Does reporting in HR require additional authorizations?

   No. The same authorization checks are performed for reporting as in dialog processing.

2. What program names may not be entered in the authorization for object HR: Reporting?

   You may never enter the name of the logical database programs (for example SAPDBPNP) because this would switch off the authorization checks for all reports that use these logical databases.

UNIT 7 Structural Authorizations

UNIT OBJECTIVES

- Outline the connection between the personnel planning data model and evaluation paths
- Outline the elements included in structural authorization profiles
- Create an overall authorization profile
- Outline authorizations for organizational objects
- Generate user authorizations using the RHPROFL0 report
- Outline the method to improve system performance for structural authorization profiles

Unit 7
Lesson 1

Outlining the Structure of the Personnel Planning Data Model

LESSON OVERVIEW
This lesson outlines the connection between the personnel planning data model and evaluation paths. This includes the set up of structural authorizations.

Business Example:

As a member of the authorizations team, you are responsible for the set up of structural authorizations which are based on evaluation paths. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline the connection between the personnel planning data model and evaluation paths

Data Model

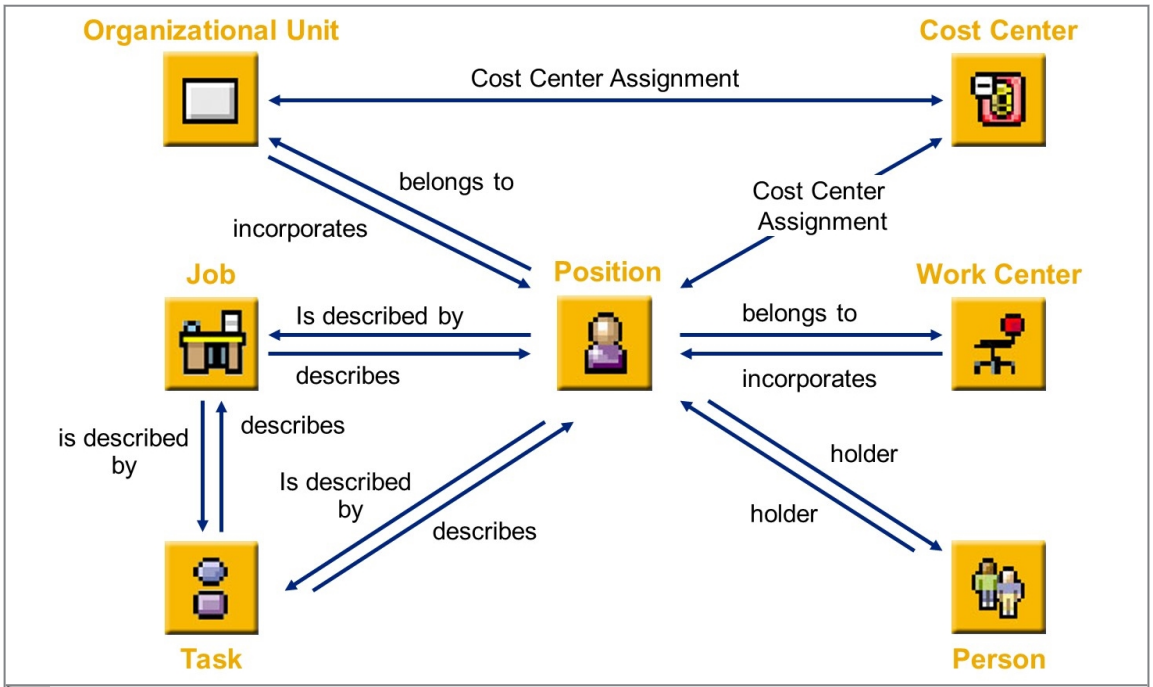

Figure 69: The Data Model for the Personnel Planning Components

The data model in Organizational Management is based on the concept that each element in an organization is represented as an independent object with individual attributes. These objects are created and maintained individually and are linked to each other using relationships to map a structure, which has the flexibility to perform personnel planning,

planning forecasts, and PA reporting. The figure titled The Data Model for the Personnel Planning Components illustrates examples of relationships between objects.

The cost center is an external object type, since it is not maintained in Organizational Management.

This data model (object types and relationships) is also the basis for other applications in Personnel Planning, such as Training and Event Management (course hierarchies) and Personnel Development (qualifications catalog).

Mapping an Organizational Structure

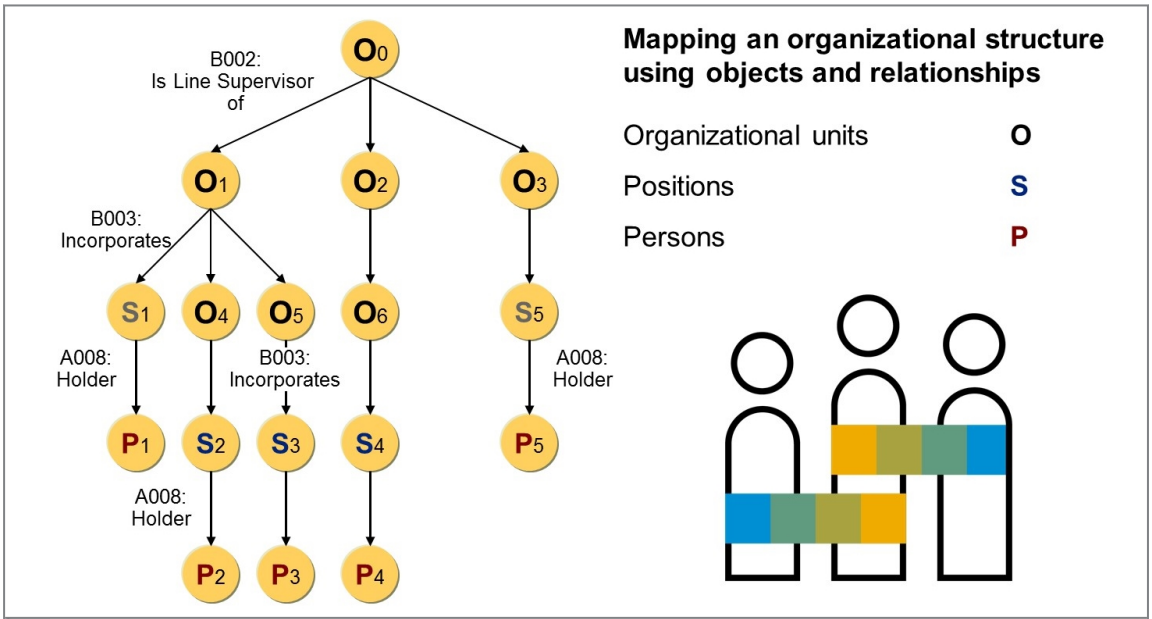

Figure 70: Mapping an Organizational Structure

Structural authorization profiles use the data model of the Personnel Planning components Organizational Management, Personnel Development and Training and Event Management to build hierarchies using objects and relationships. Different types of objects (object types) and different types of relationships are used in this process. The organizational structure of a company is mapped as shown in the figure Mapping an Organizational Structure.

To manage the authorizations for this model effectively, the central elements of this data model are used. These elements include objects, relationships, and evaluation paths.

Evaluation Paths

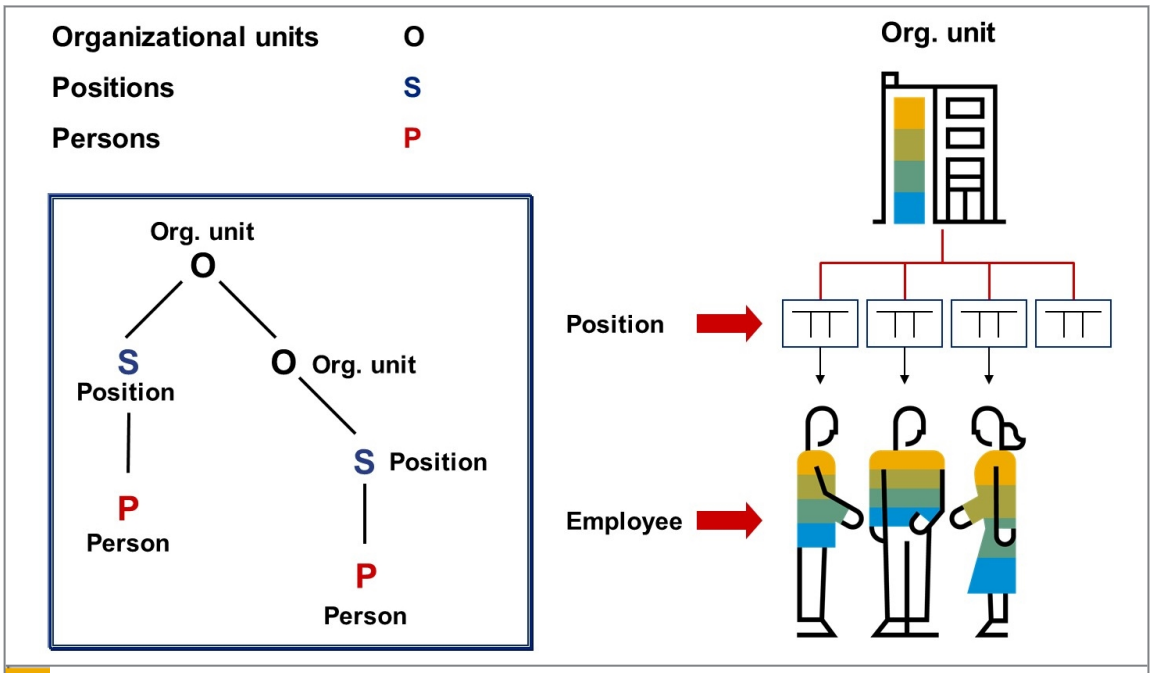

Figure 71: Evaluation Paths

An evaluation path describes a chain of relationships that exist between objects in a hierarchical structure. The evaluation path O-S-P, for example, describes the relationship chain organizational unit to position to person.

Evaluation paths “collect” objects from a start object in an existing structure according to their definition. The definition of an evaluation path determines the start object and which object types using which relationships are selected.

The Evaluation Path O-S-P

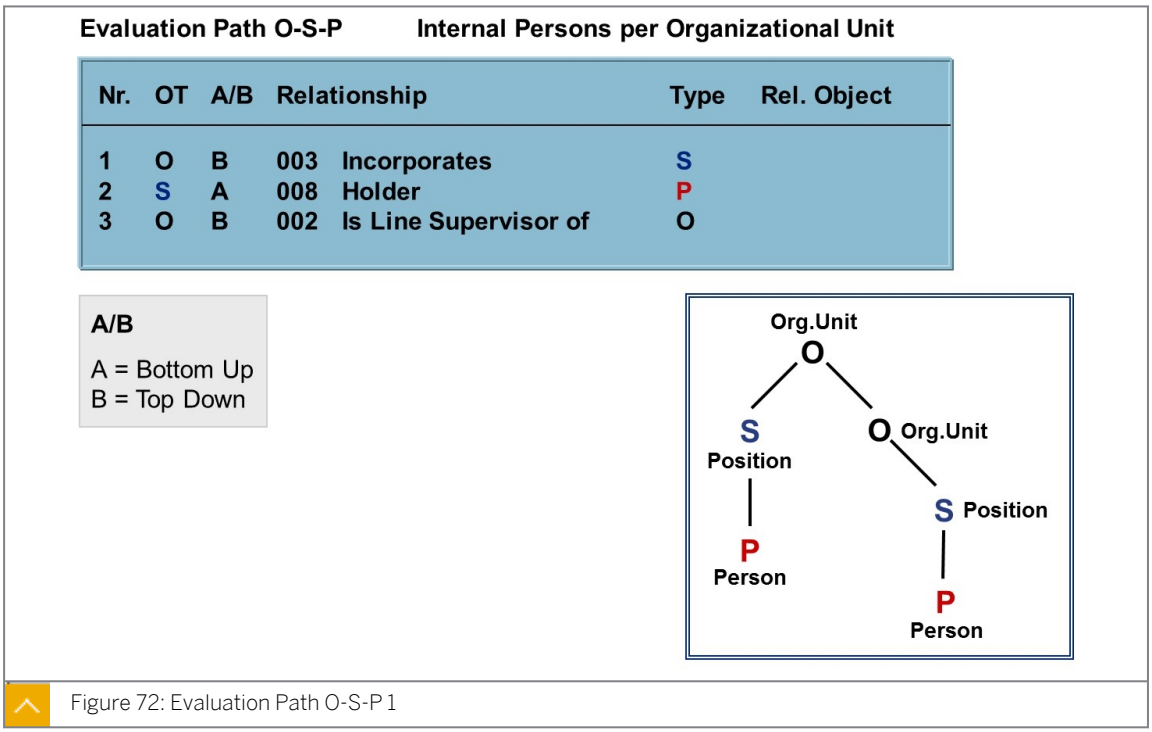

Figure 72: Evaluation Path O-S-P 1

An example of an evaluation path is O-S-P. In this evaluation path, each assigned position (S) and its holder (P) is determined for a specified organizational unit (O). The lower-level organizational units are processed in a similar way. The O-S-P evaluation path is a standard evaluation path that plays a central role in authorizations.

The naming convention A = bottom up and B = top down can be taken in account when a relationship is defined for the first time. However, this convention is not a compulsory rule.

Evaluation Path O-S-P 2

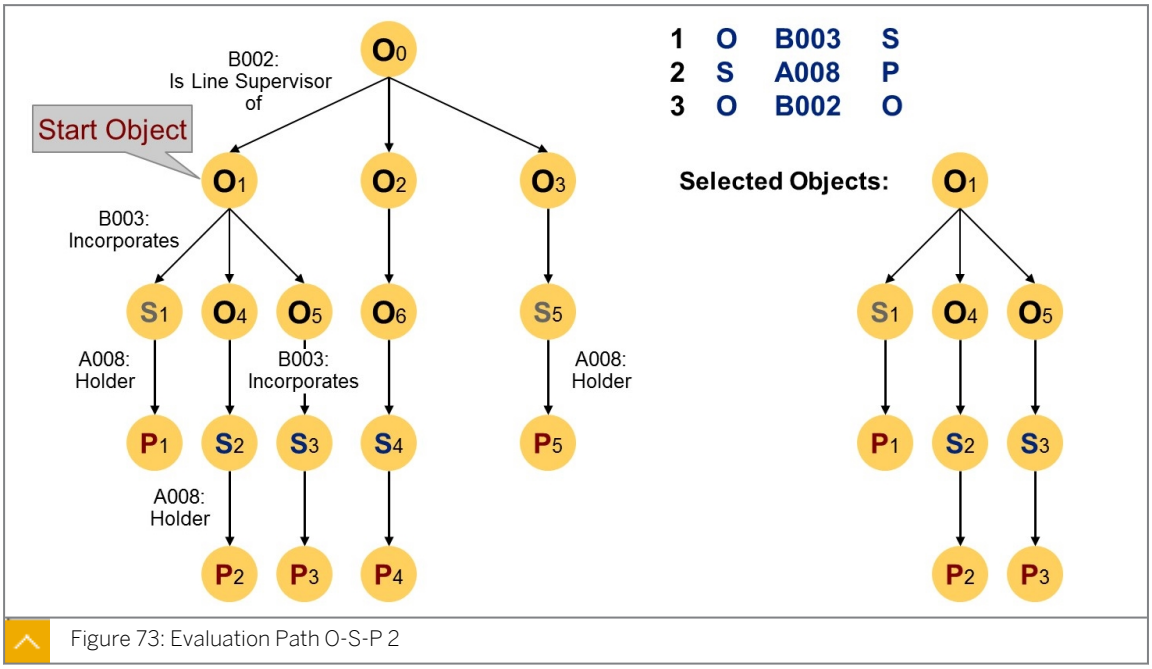

Figure 73: Evaluation Path O-S-P 2

This evaluation path starts selection from an organizational unit (O) that is used as the start object (the organizational unit O1 is used in the following example). The evaluation path first selects all positions from row 1 of the definition. The above position is selected for the structure in the example: S1.

Secondly, all persons are selected, starting with the positions chosen, according to row 2 of the definition. In the example: P1.

Thirdly, all the subordinate organizational units are selected.

A combination of start object and evaluation path returns a specific number of objects from an existing structure. This exact combination, that is, the set of objects returned by this combination, represents a user's structural profile. Note that neither the number of objects nor the specific objects that are returned by a structural profile are constant, nor is this desirable. The concrete objects that are returned by a structural profile change as the organizational structure (under the start object) changes.

LESSON SUMMARY

You should now be able to:

- Outline the connection between the personnel planning data model and evaluation paths

Unit 7
Lesson 2

Outlining Structural Authorization Profiles

LESSON OVERVIEW
This lesson outlines the elements included in structural authorization profiles.

Business Example

Managers in your company may be responsible for the management of different organizational units. The access they have to information depends on the organizational unit. Structural authorization profiles are required to enable managers to access selected HR data of the employees within their span of control. As the authorization administrator, you are responsible for the set up of appropriate authorizations. To accomplish this task, you require the following information:

- An understanding of structural authorizations

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline the elements included in structural authorization profiles

Structural Authorization Profiles

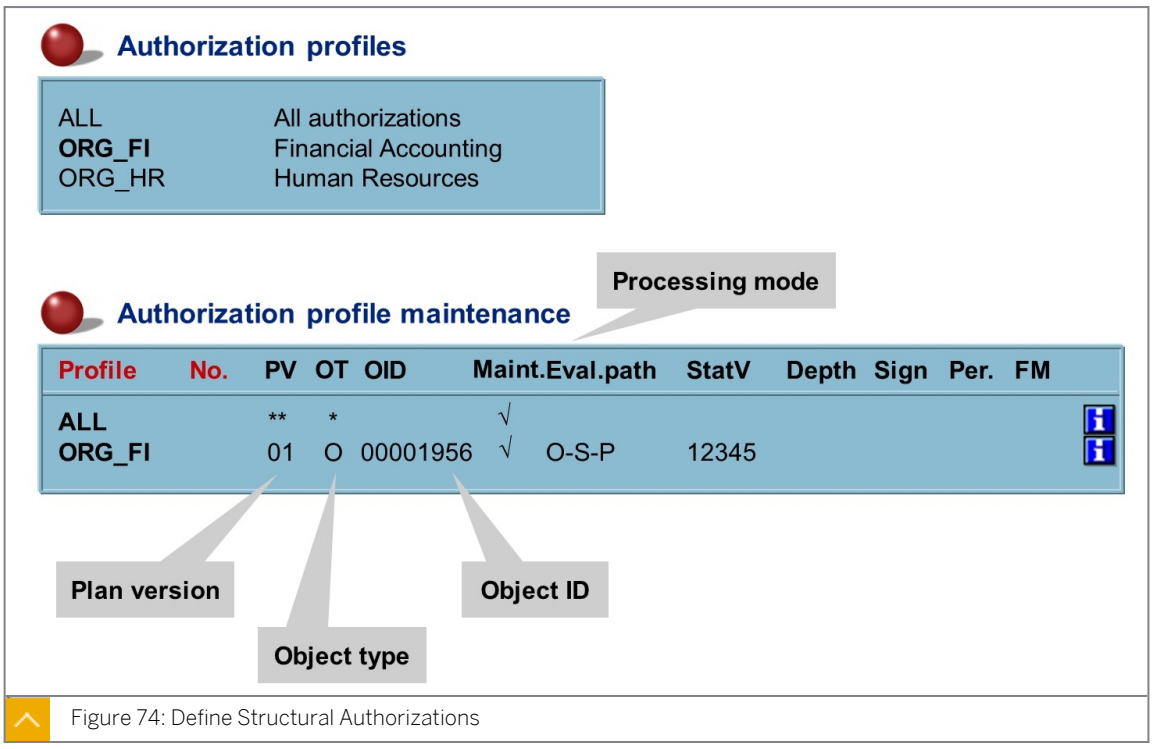

Figure 74: Define Structural Authorizations

You use the *Plan version* field to determine the plan version to which the defined profile applies. If you use a system that integrates the Personnel Administration and Organizational Structure components, note that plan version 01 is generally the integrated plan version.

In the *Object type* field, specify only object types that have an eight-digit key. In general, structural authorization checks are not carried out for external objects with a different key (for example, cost centers).

In the *Object ID* field, enter the number of the start object if you are using evaluation paths.

Use the processing mode to control whether a read authorization or maintain authorization for the relevant set of objects should be assigned. This field corresponds to the *MAINT* field in table T77FC. All function codes that have “X” in this field can be processed.

By entering a specific evaluation path, you can determine that the user is only authorized to access objects along this evaluation path. You must also assign a root object for the structure when you use an evaluation path. This root object can either be entered directly in the *Object ID* field or determined dynamically by a suitable function module.

Only use the *Sign* field if you want to create structural authorization profiles that process the structure “bottom up”.

The Status Vector in Relationships

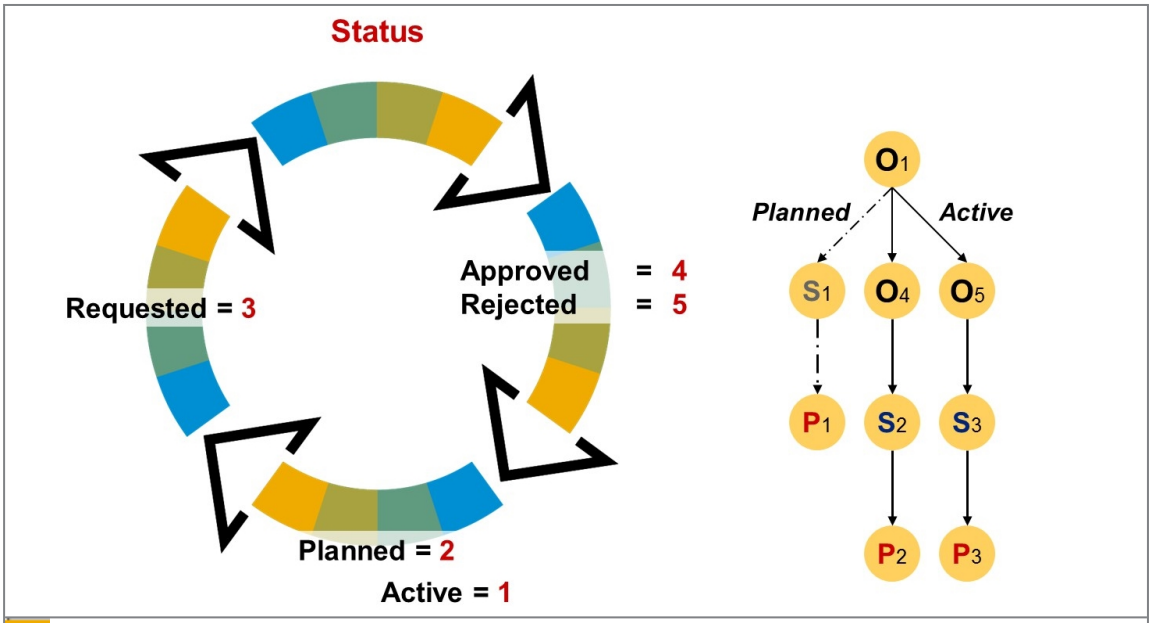

Figure 75: The Status Vector in Relationships

Use the status vector to determine which relationships are considered when the structure is created. If you define the status vector as 12, for example, all relationships that have the status *active* and *planned* are evaluated. The choice of status vector has no real effect on the status of objects. The status vector simply refers to the status of the relationships.

Display Depth

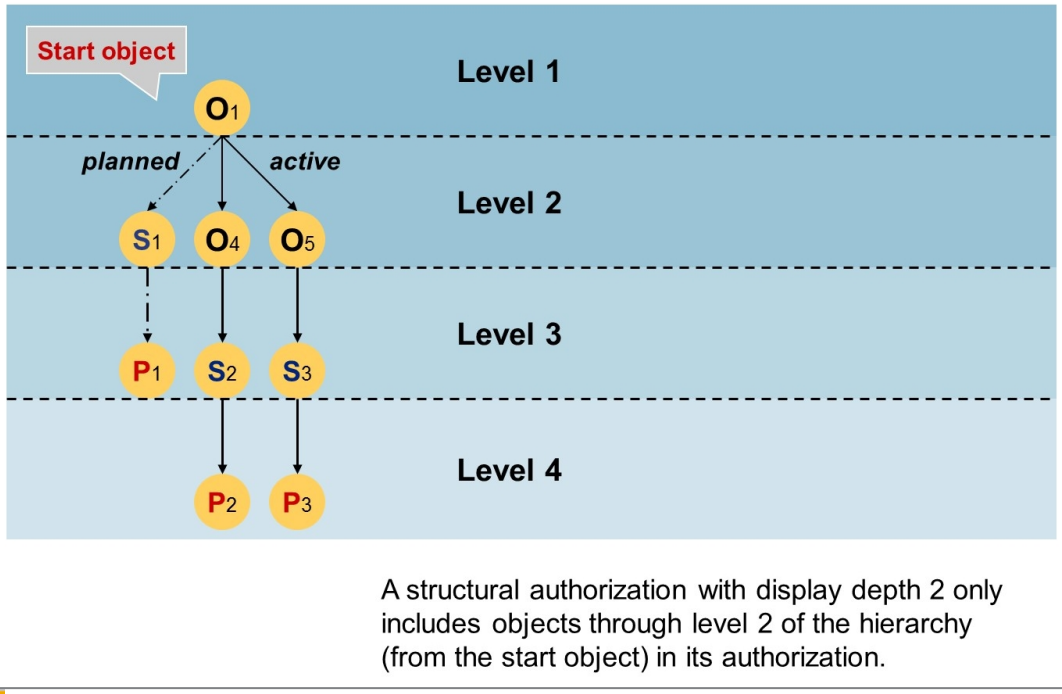

Figure 76: Display Depth

If you enter 0 as the value for the display depth, the corresponding tree is completely built. There is no limit to the depth of the tree.

Sign

If the field *Sign* is not pronounced, the structure is always evaluated from top to bottom.

The - sign can be used to process the structure from bottom to top. In the example above the structural authorization will only include objects in level 4 and level 3.

Period

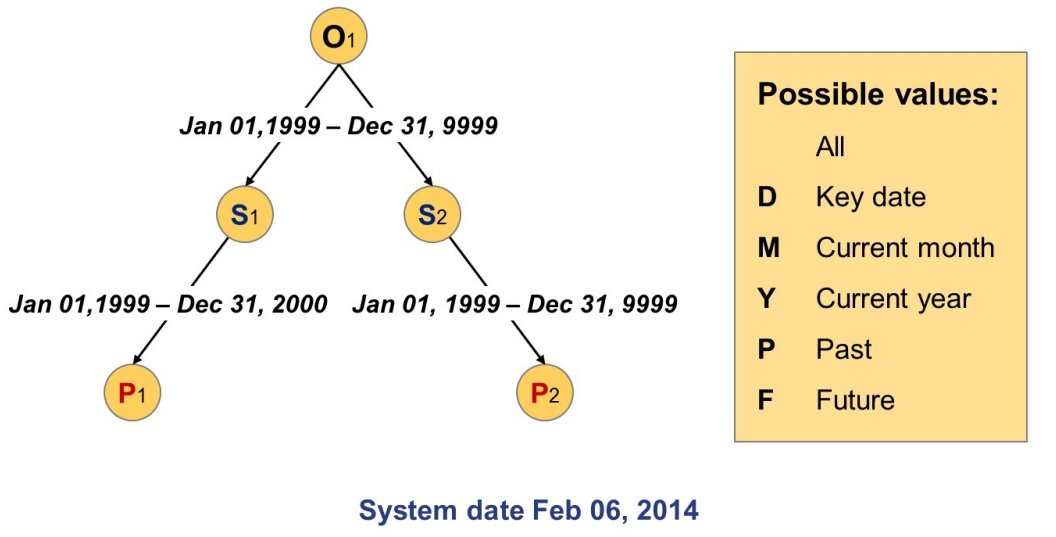

Figure 77: Period

This parameter is used to define the profile according to the validity period of the structure. The parameter has no influence on the period for which a user is authorized to access a given object. Unlike the general authorization check, the structural authorization check does not return periods of responsibility. Instead, the system indicates whether or not the user has authorization for a specific object.

If you select **D** (current day) for example, the structural authorization is extended to include only the structures valid on the current day. If you define a structural authorization like this for a manager, the manager is authorized to access data for all persons who are currently in his or her organizational unit.

If you do not make an entry, there is no restriction by validity period of the structures. In this case, the manager is authorized to access data on former or future employees in addition to the authorization in the previous example.

For the following examples, assume the system date is **February 6, 2014**:

Example 1: If you enter the value D, the user is only authorized to access P2. Since the user in this case only has authorization for objects in the structure valid on February 6, 2014 and since the relationship between S1 and P1 ends before February 6, 2014, the user is not granted access to P1.

Example 2: If you enter the value BLANK, the user is authorized to access P1 and P2.

Function Module

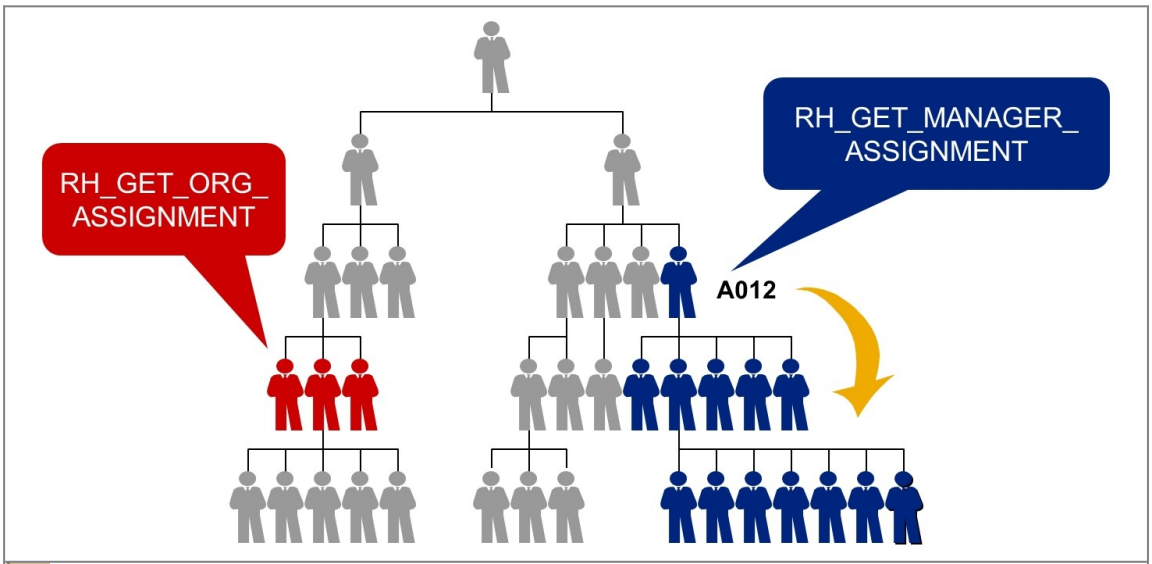

Figure 78: Function Module

When you define a structural authorization, you can specify a function module, which dynamically determines a root object during runtime.

In the area in which you have specified the organizational assignment to be determined dynamically, do not make an entry in the *Object ID* field of the structural authorization. However, make sure you enter a plan version and an object type.

The advantage of using function modules is that a user-specific profile is created by the dynamic definition of a root object at runtime. If a manager changes departments, for example, the corresponding profile does not need to be changed. The number of structural authorizations can be significantly reduced by using function modules.

There are two function modules in the standard system:

- RH_GET_MANAGER_ASSIGNMENT (Determine Organizational Units for Manager). This function module determines the root object of the organizational unit to which the user is assigned by the A012 relationship (manages). This function module works on the basis of a key date and can determine only the organizational units assigned to the user as manager on the key date or within the specified period.
- RH_GET_ORG_ASSIGNMENT (Organizational Assignment) This function module determines the organizational unit assigned to the user organizationally as the root object.

Examples of Structural Authorization Profiles

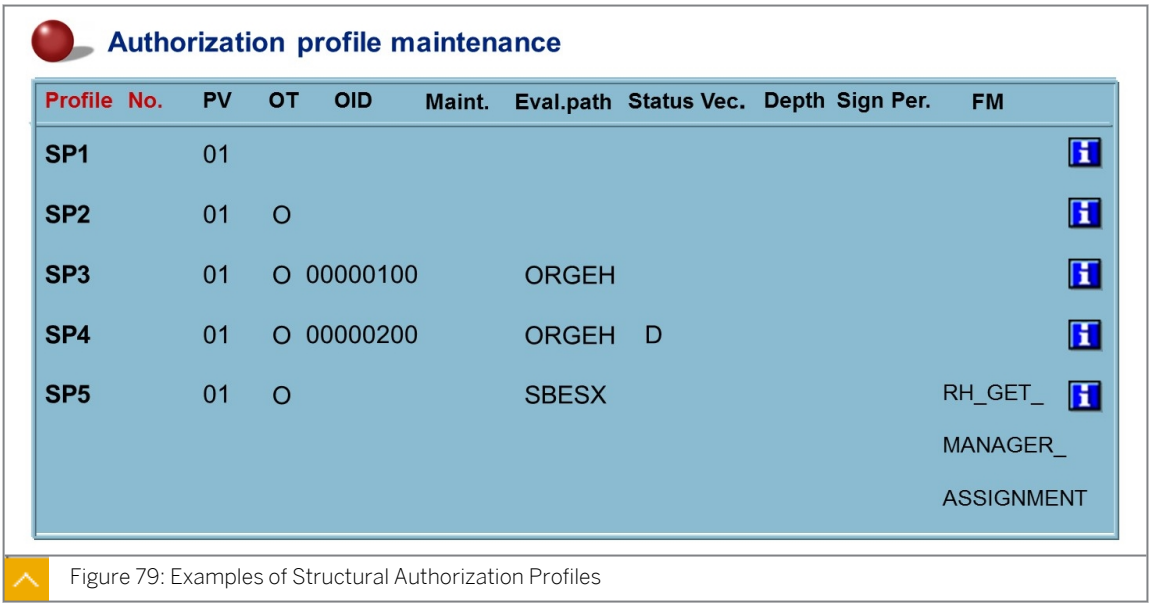

Figure 79: Examples of Structural Authorization Profiles

Example 1: Profile SP1: Due to the user's authorization profile, the user is authorized to access plan version "01".

Example 2: Profile SP2: Due to the user's authorization profile, the user is authorized to access organizational units in plan version "01"

Example 3: Profile SP3: Due to the user's authorization profile, the user is authorized to access organizational units in plan version "01" from a root object (entry in the *Object ID* field) along the "Organizational Structure" evaluation path.

Example 4: Profile SP4: Due to the user's authorization profile, the user is authorized to access organizational units in the structure valid on the current day in plan version "01" from root object 200.

Example 5: Profile SP5: Due to the user's authorization profile, the user is authorized to access objects in plan version "01" from a root object along the Staffing Assignments Along Organizational Structure evaluation path. The root object is determined in this case using the function module. No entry should be made in the Object ID field. The user is then granted access authorization to the organizational unit he or she manages and to all lower-level objects along the SBESX evaluation path.

Show Authorization Views

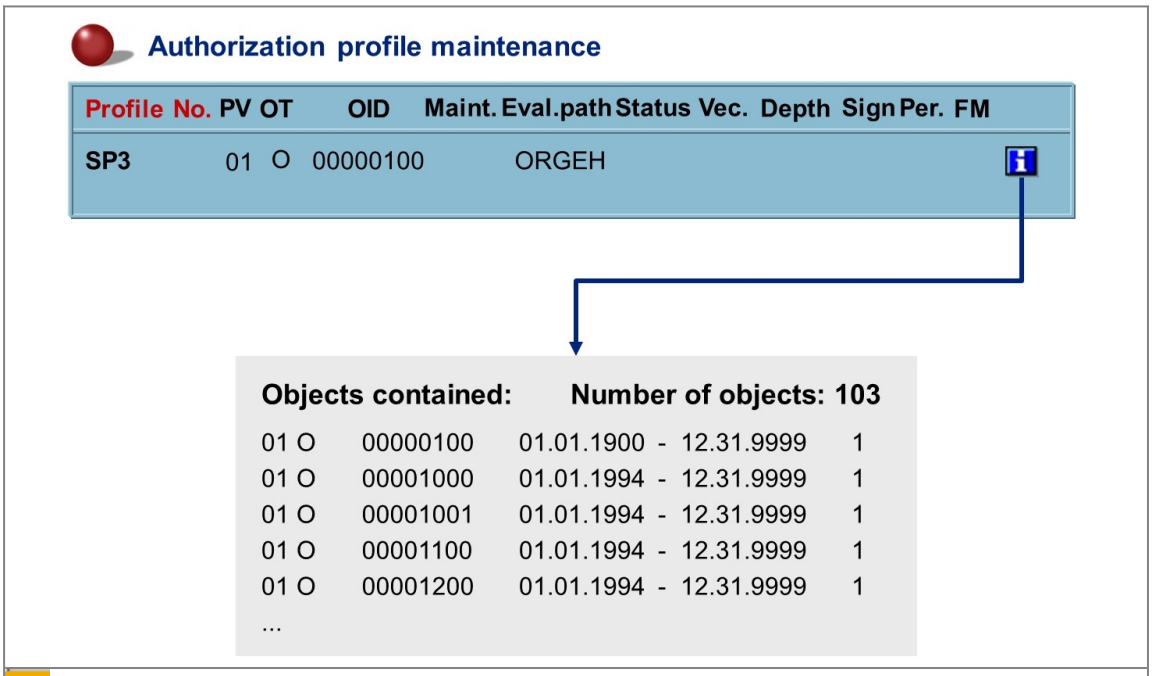

Figure 80: Show Authorization Views

You can call the RHAUTH01 report by clicking *Info*. This program lists the objects contained in the structural authorization.

Assignment of Structural Authorizations

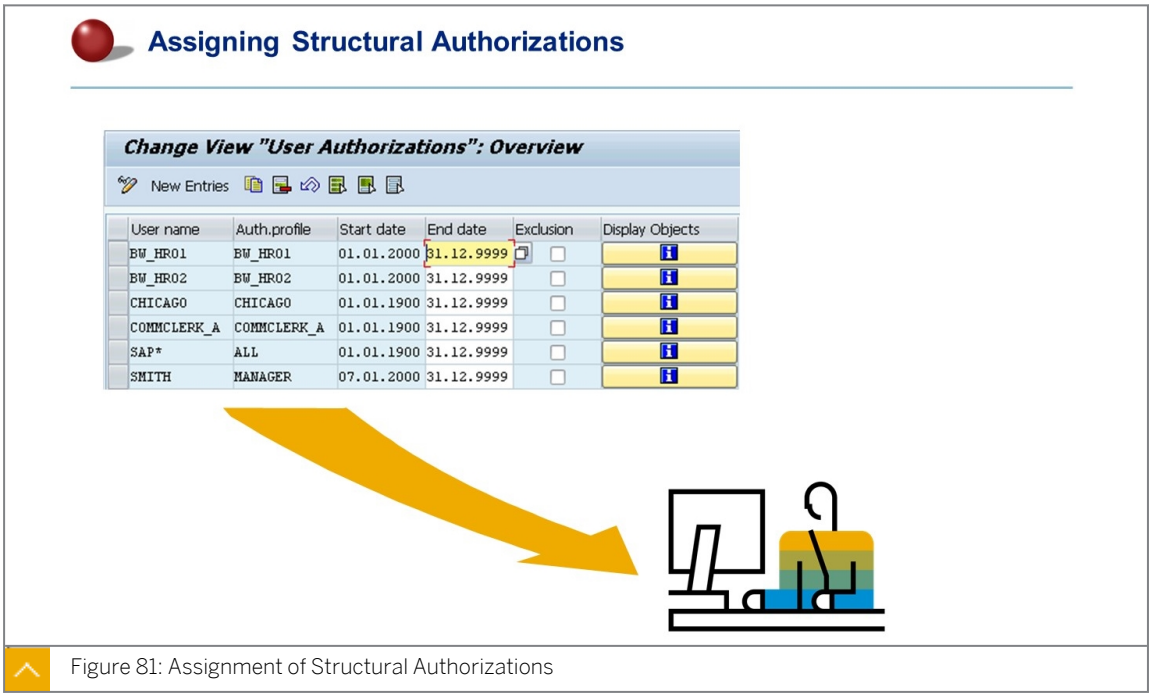

Figure 81: Assignment of Structural Authorizations

Structural profiles are assigned in a different way than general authorization profiles. To assign structural profiles, you use table T77UA and not the Profile Generator (transaction code PFCG) as with general authorization profiles.

First, the system searches at runtime for entries in table T77UA for the current user. If one or more entries exist, the set of objects is mapped according to the profile definition. The set of objects is then checked against the concrete object and the action (Display or Edit). The authorization is granted only if the object to be checked exists with the necessary processing indicator in the set of objects.

Note:
If table T77UA does not contain an entry for the current user, the above check is made in the same way for the entry *SAP** in table T77UA. If still no entry exists, the authorization is denied. In the standard system, there is an entry for user *SAP** with the profile ALL. This means that when you first implement the HR components, all users have complete authorization as far as structural authorization is concerned.

You can edit this table in Customizing by choosing: Personnel Management > Organizational Management > Basic Settings > Authorization Management > Structural Authorization > Assign Structural Authorization.

LESSON SUMMARY
You should now be able to:

- Outline the elements included in structural authorization profiles

Unit 7
Lesson 3

Creating Overall Authorization Profiles

LESSON OVERVIEW

LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Create an overall authorization profile

Overall Authorization Profile

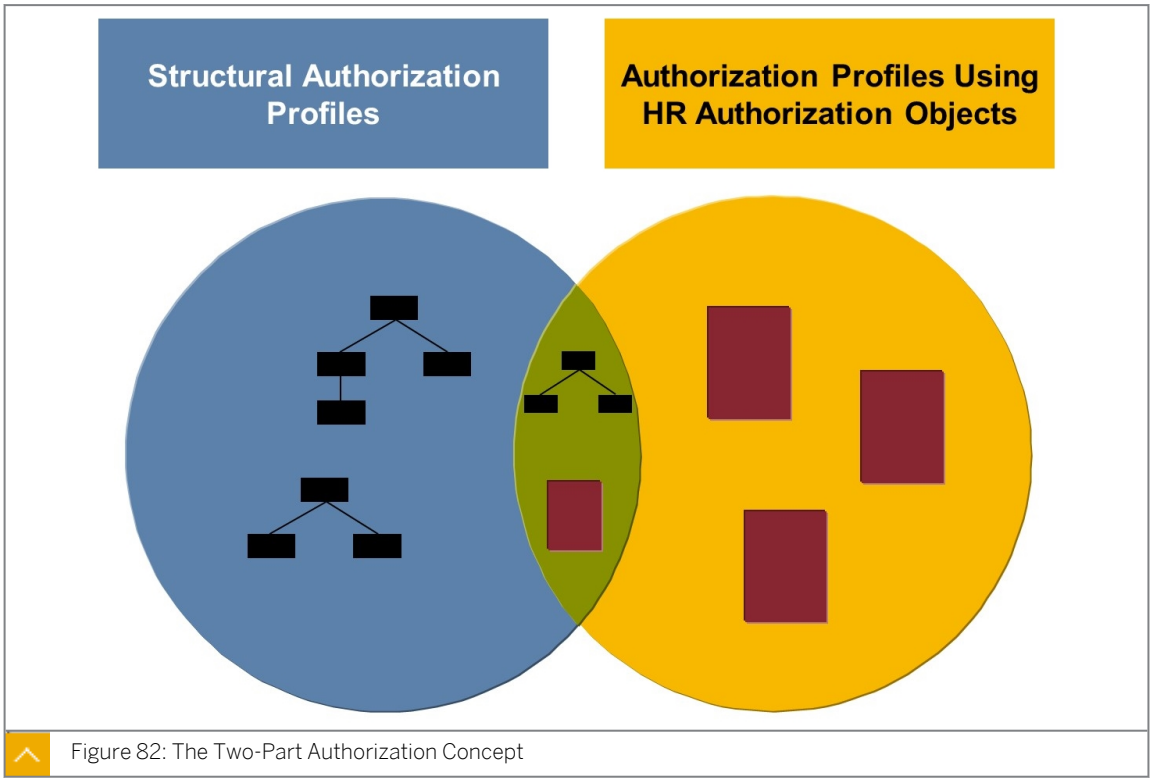

Figure 82: The Two-Part Authorization Concept

If you use both structural and general authorizations, a user's overall profile is determined from the intersection of the structural and general authorization profiles of the user.

The structural profile determines which objects in the organizational structure the user may access. The general profile determines which data (infotype, subtype) and which access mode (read, write) the user has for these objects.

Overall Authorization Profile

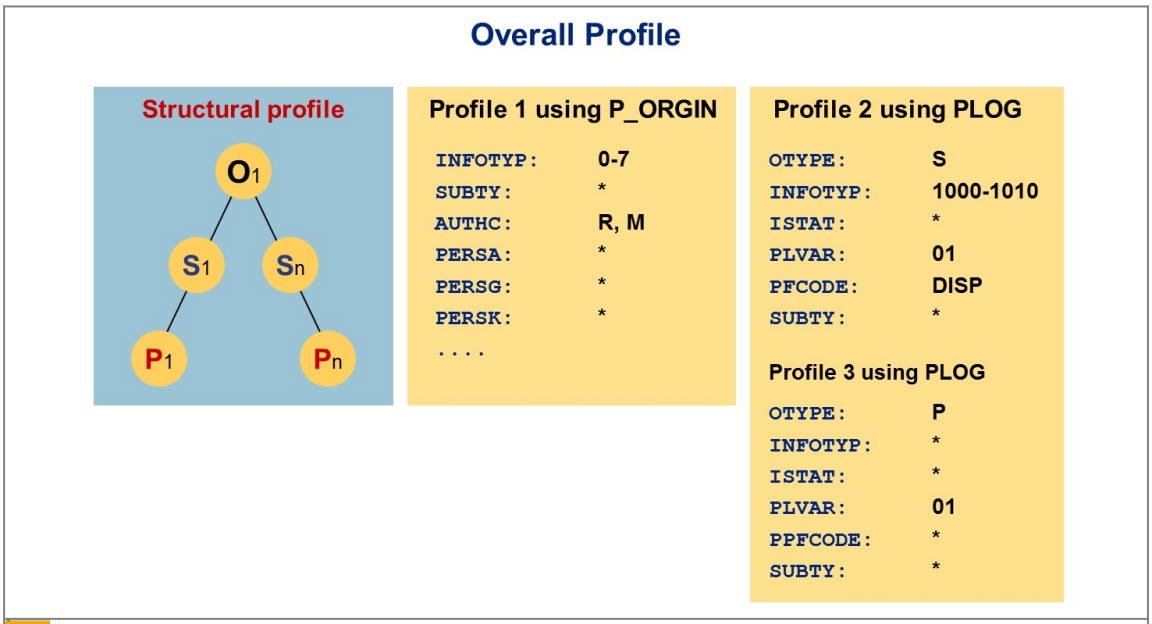

Figure 83: Overall Authorization Profile

The following authorizations or restrictions apply to a user who has the overall profile shown in the figure titled Overall Authorization Profile:

The user has read authorization for positions S1 to SN in infotypes 1000 to 1010 (structural profile and profile 2 using PLOG).

The user is not authorized to access organizational units with this profile since the user has no corresponding PLOG authorization.

The user has read authorization for persons P1 to PN in infotypes 0000 to 0007 (structural profile and profile 1 using P_ORGIN). The period of responsibility for persons is also determined accordingly.

For the user to be able to access data on persons, you need to assign the user a corresponding PLOG authorization for persons. The infotype does not have to be specified (Profile 3 using PLOG).

Period of Responsibility According to the Structural Authorization Check

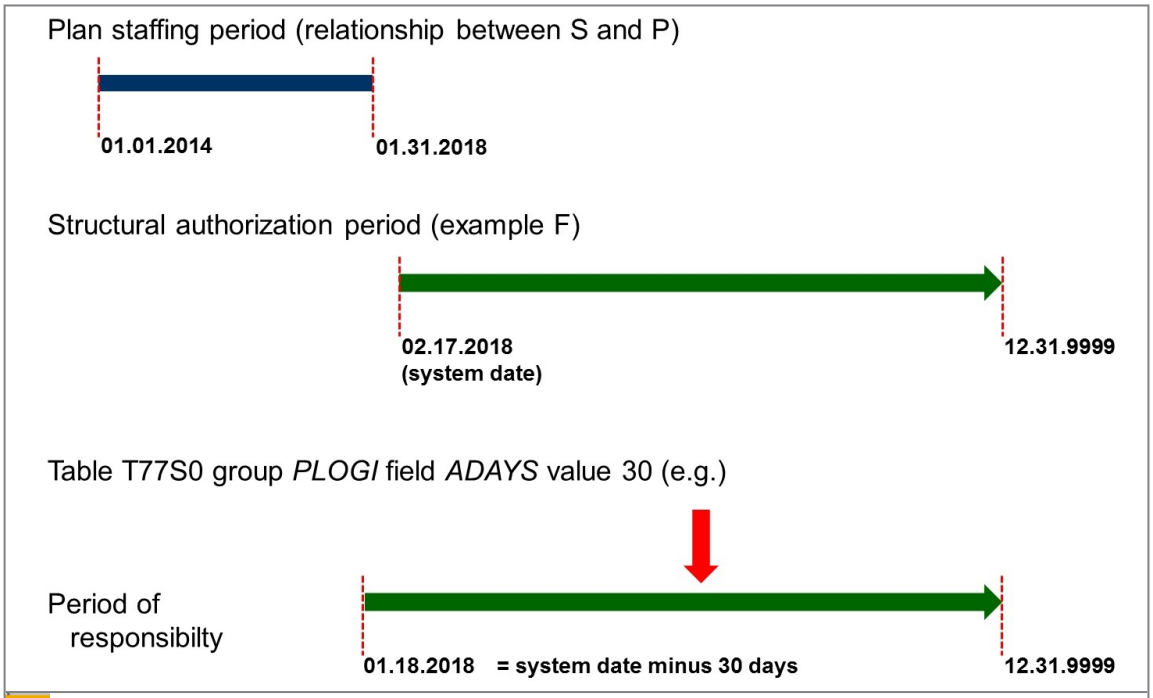

Figure 84: Structural Authorizations Period of Responsibility

The period check of the structural authorization takes place before the period check of the general authorization.

The period of responsibility of the structural authorization results from the last plan staffing period (relationship between S and P).

In the example above, the structural authorization period is F (Future). Therefore, the period of responsibility starts at the system date and extends to the high date. There is no overlap between the plan staffing period and the structural authorization period. The period of responsibility is empty.

In the example the field *ADAYS* in group *PLOGI* of table T77S0 contains 30 (days). In this case the period of responsibility begins 30 days before the system date and overlaps with the plan staffing period.

The period of responsibility is then transferred to the general authorization and processed in the time logic.

Flowchart: Overall Authorization

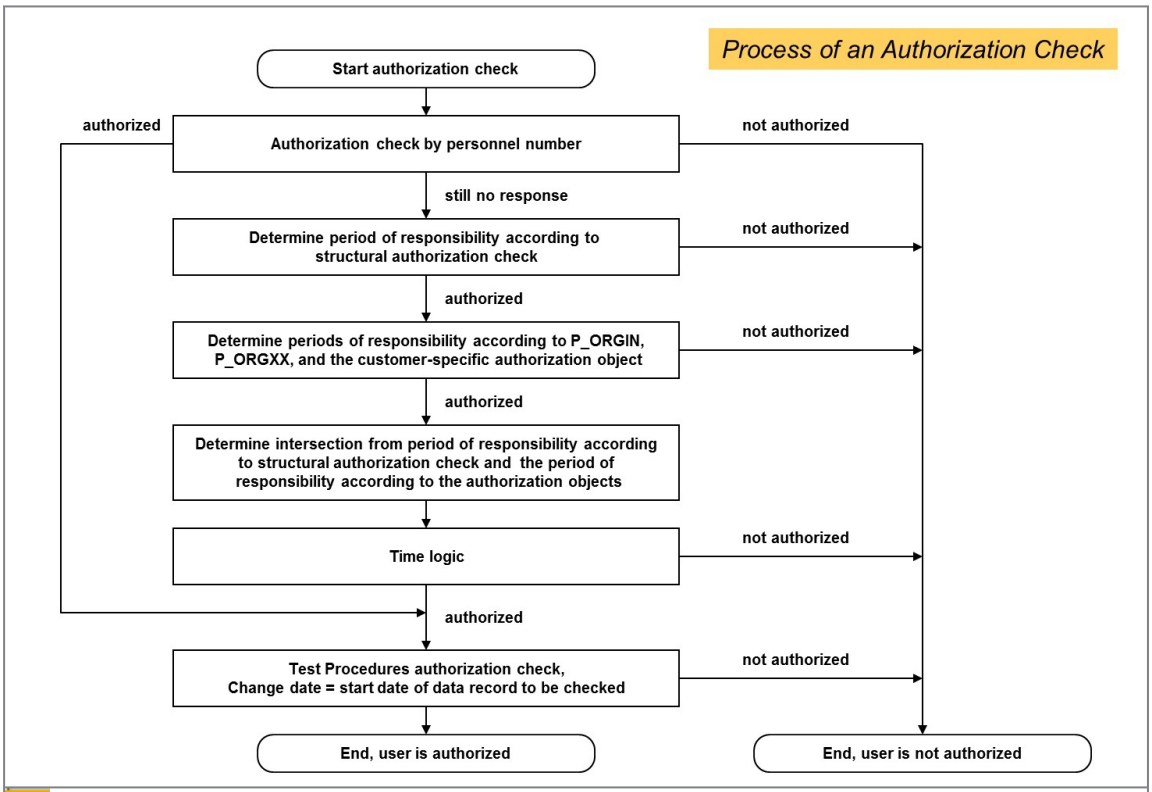

Figure 85: Flowchart: Overall Authorization

The flowchart illustrates the process of an authorization process.

LESSON SUMMARY

You should now be able to:

- Create an overall authorization profile

Unit 7
Lesson 4

Generating Authorizations

LESSON OVERVIEW
This lesson outlines the process of assigning authorizations for organizational objects and using the RHPROFL0 report to create authorization profiles for users within an organizational plan.

Business Example:

You are responsible for the set up of authorizations for organizational objects. You plan to use the RHPROFL0 report to create authorization profiles for users within an organizational plan. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline authorizations for organizational objects
- Generate user authorizations using the RHPROFL0 report

Authorizations for Organizational Objects

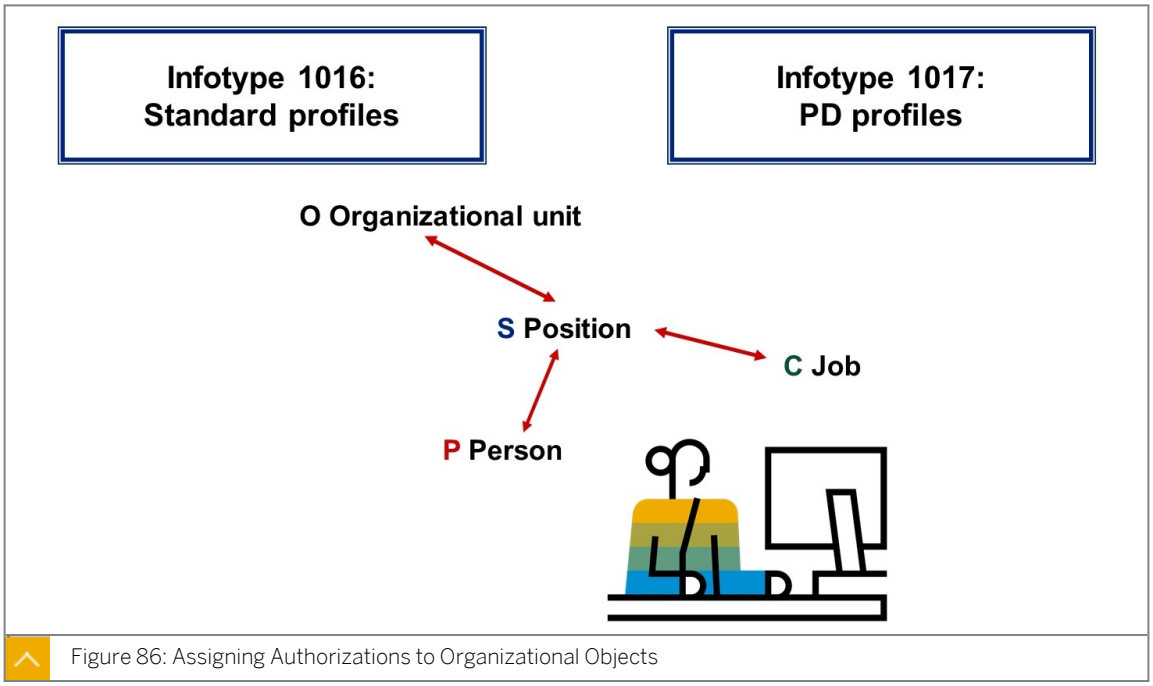

Figure 86: Assigning Authorizations to Organizational Objects

The *PD Profiles* and *Standard profiles* infotypes allow you to link authorization profiles with the following objects: organizational units, jobs, positions, and tasks (or standard tasks if your company uses Workflow Management). The profiles related to organizational units, jobs,

positions, or tasks are used for all employees linked with these objects when you run the RHPROFL0 report.

In the *PD Profiles* infotype (1017), specify the structural authorization profiles that you want to relate with a task, job, position, or organizational unit. If, for example, the authorization profiles for all employees of an organizational unit tend to be fairly similar, it may be most effective to use profiles for entire organizational units. If, however, authorizations vary by job or task, it may be better to use the profile for the job or task concerned.

The *Standard Profiles* infotype (1016) enables you to assign a **manually** created authorization profile to an organizational unit, job, or position, and so on. You should not enter authorization profiles in this infotype that you created for a role using the Profile Generator. Assign the generated profiles to Organizational Management using role maintenance (transaction PFCG).

Authorization Report RHPROFL0

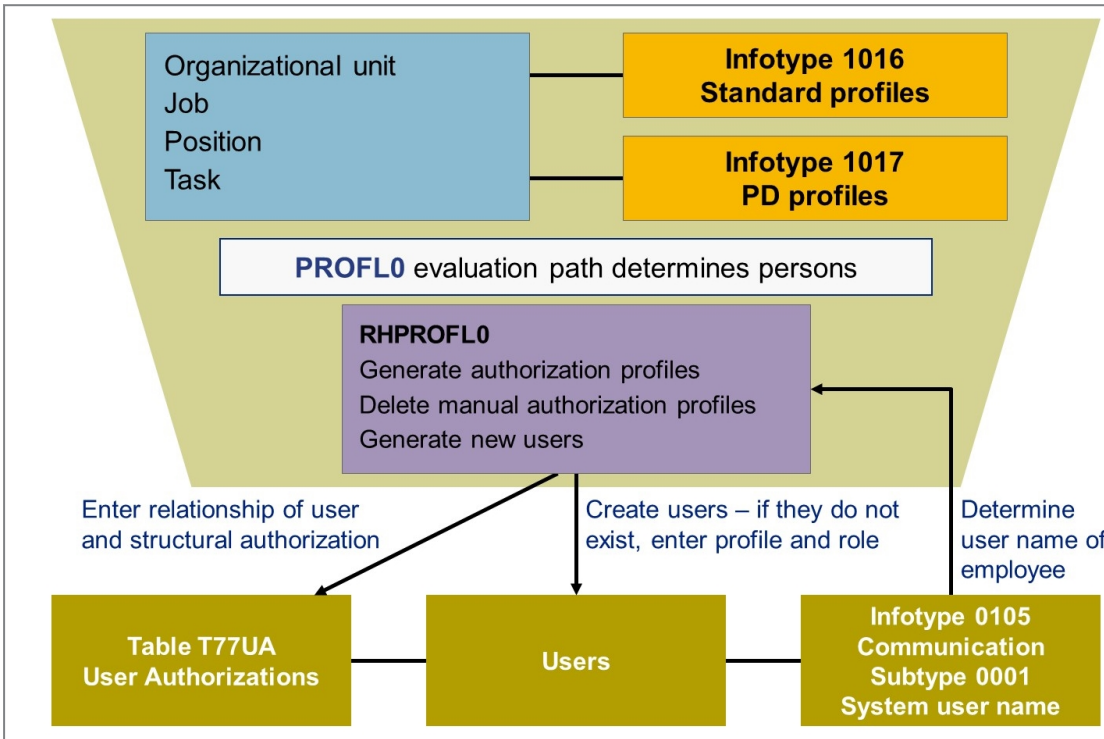

Figure 87: The RHPROFL0 Report (1)

The *RHPROFL0* report creates authorization profiles for a user within an organizational plan. The report differentiates between standard authorization profiles and authorization profiles for structural PD authorizations. When authorization profiles are generated using the Profile Generator, the user is also assigned user roles that are linked to the profile.

The system searches along the *PROFL0* evaluation path for all persons in the structure and saves them temporarily. Using these persons as a basis, the system reads, up to the next higher organizational unit, all related objects for a given key date that are valid at this time and have infotype 1016 and/or 1017 appended.

The system then checks whether users already exist in the system for the persons found. This is necessary because users also created in the system cannot be entered in infotype 0105 (subtype 0001) for the person.

If the user has not yet been created in the system, it is created automatically. The authorization profiles for all users found in the organizational plan are then entered.

You can check the results of the standard authorization profiles and user roles with transaction *SU01*. The structural PD authorizations can be displayed using transaction *OOSB*.

The RHPROFL0 Report (2)

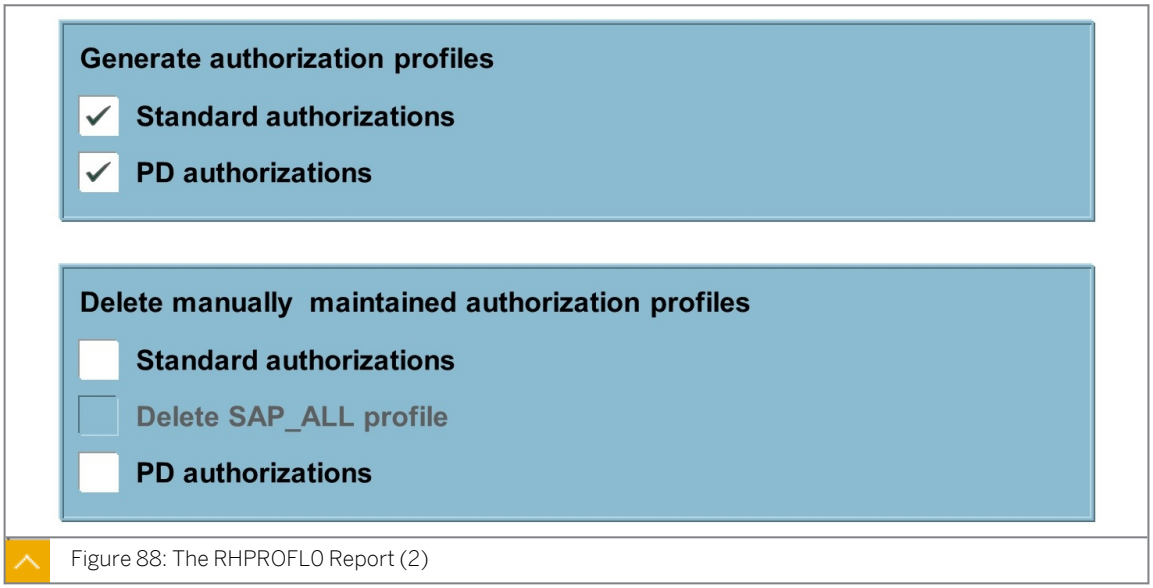

Figure 88: The RHPROFL0 Report (2)

If the *Generate standard authorizations* parameter is set, the corresponding standard authorization profiles are changed. The same applies to the *Generate PD authorizations* parameter and the structural PD authorization profiles. If the appropriate parameter is not set, the authorization profiles assigned to the users remain unchanged.

Caution:
If the *Delete standard authorizations* parameter is set, the system deletes all profiles maintained manually for the user through transaction *SU01*. It only reassigns the new authorization profiles derived from the organizational plan. An exception is the *SAP_ALL* profile. If you want this profile to be deleted as well, you must set the *Delete SAP_ALL profile* parameter.

If the parameter is not set (default setting), the system only deletes those authorization profiles resulting from a user role that - according to the current organizational plan - is no longer assigned to the user. These authorization profiles are also flagged as generated profiles in transaction *SU01*. All other authorization profiles that were maintained manually (infotype 1016) remain.

Caution:
If the *Delete PD authorizations* parameter is set, the system deletes all structural PD authorization profiles that were maintained manually in table *T77UA* . Note that a user who has no structural authorization profiles automatically receives the *SAP** authorization profile. However, this profile is not entered in table *T77UA*. If the parameter is not set (default setting), the system only deletes authorization profiles that were previously assigned by report *RHPROFL0*.

The RHPROFL0 Report (3)

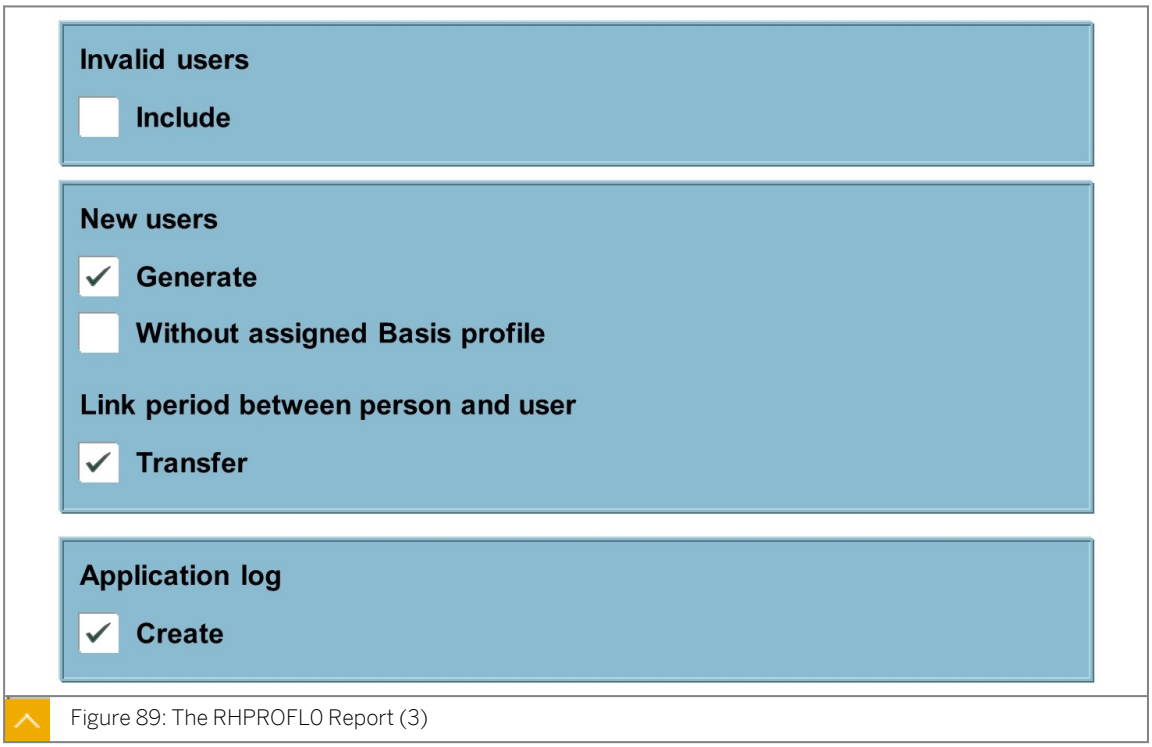

Figure 89: The RHPROFL0 Report (3)

If the *Include invalid users* parameter is set, the system also selects those users who are no longer valid on the key date, but who still exist in the system.

If the *Generate new users* parameter is set, the system generates users that are assigned to a person in infotype 0105 (subtype 0001) but not yet created in the system. If the Transfer relationship period between person and user parameter is also set, the system creates the new user with the same validity period that is maintained for the person in infotype 0105 (subtype 0001). If this parameter is not set, the system creates the user with a validity period from the key date until the latest possible date (12.31.9999). If you have not stored any authorization profiles in the *Standard Profiles* infotype (1016), you must activate the parameter *Without assigned basis profiles*. You use the parameter *User Data* to assign the *initial password* and the *user group*.

All messages that were generated during the profile comparison are saved in an application log. This application log is newly generated each time the RHPROFL0 report is run. You can make it visible by choosing *Display log(s)*.

If the report is planned and automatically executed in a batch job, the output list is printed out. In this case, you can make the application log visible using transaction *SLG1*. On the selection screen, enter RHPROFL0 in the *Object* field. The *Subobject* and *Ext. number* fields remain empty.

LESSON SUMMARY

You should now be able to:

- Outline authorizations for organizational objects
- Generate user authorizations using the RHPROFL0 report

Unit 7
Lesson 5

Improving System Performance for Structural Authorization Profiles

LESSON OVERVIEW
This lesson outlines how you can improve system performance for structural authorization profiles.

Business Example:

You are responsible for structural authorizations and would like to use indexes for structural authorization profiles. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline the method to improve system performance for structural authorization profiles

Indexes for Structural Authorization Profiles

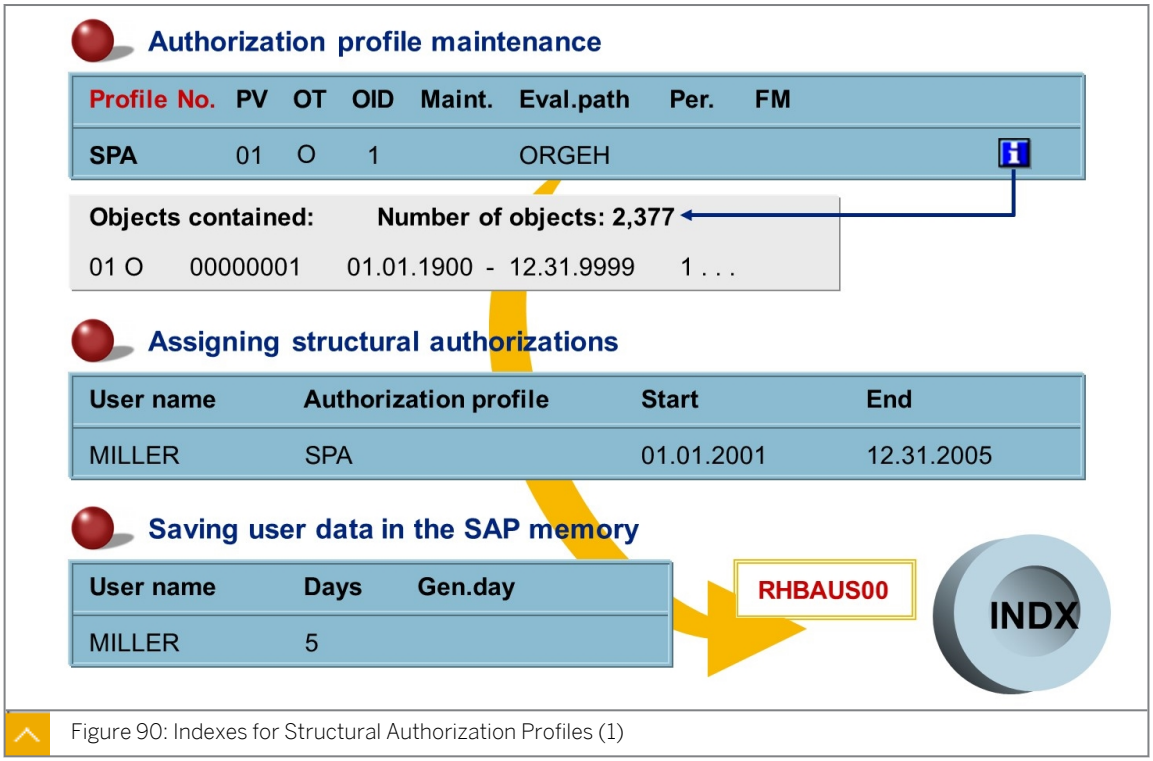

Figure 90: Indexes for Structural Authorization Profiles (1)

If you have created structural authorizations with a large number of objects, it is advisable for performance tuning reasons to generate indices for users assigned to these structural authorizations. You can do this using the RHBAUS00 report.

Before you can run this report, you should have specified in table T77UU (User Data in SAP Memory) which users' structural authorization data should be permanently stored in the SAP memory and how often the data should be refreshed (*Days* field).

There are two possible ways to fill the index with data:

1. The index can be filled automatically at fixed intervals. In this case, you have to ensure that the user's view is up-to-date on a daily basis because data is refreshed after a batch input session that runs at night.
2. The index can be filled manually by means of the report. This report updates the data in the SAP memory immediately.

Once the report has been run, you obtain a log that contains a list of the users whose index was regenerated and the number of objects that were included in the index for a user.

Indexes for Structural Authorization Profiles (2)

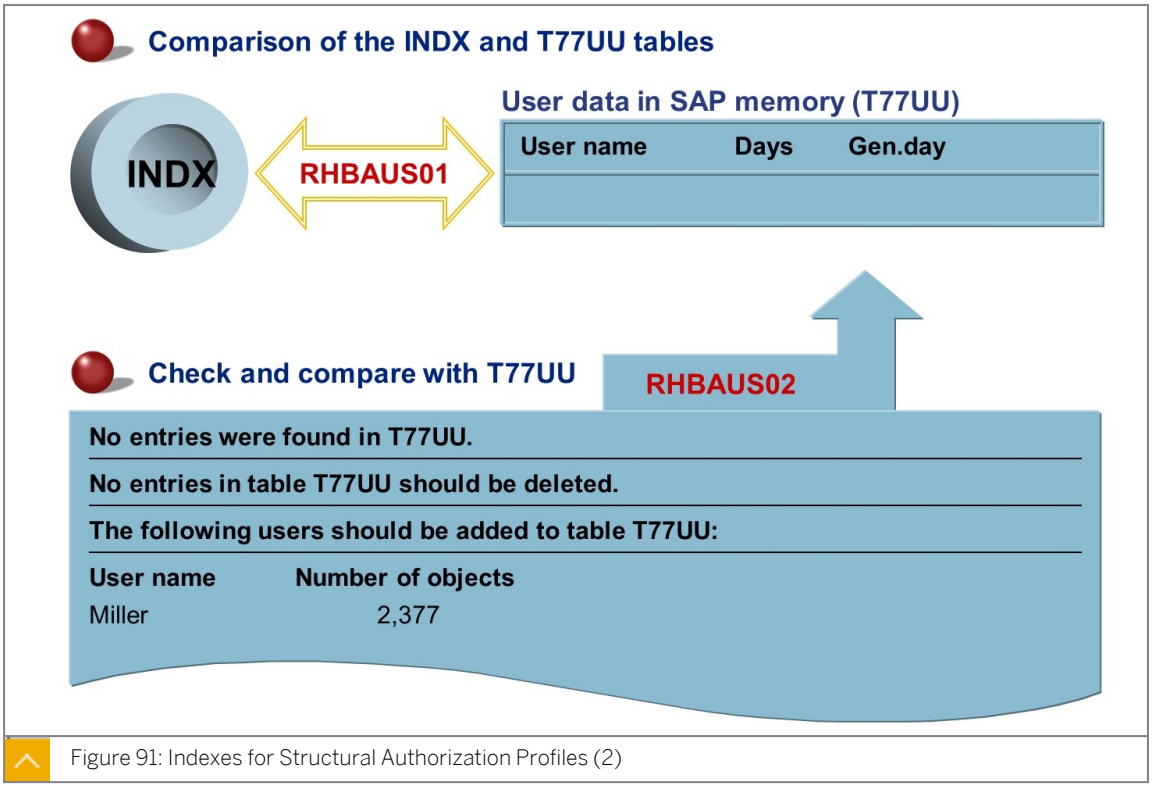

Figure 91: Indexes for Structural Authorization Profiles (2)

You can use the RHBAUS01 report to compare the INDX and T77UU tables (*Save User Data in SAP Memory*). This report generates a list of users who have structural authorization data in the SAP memory, but who are no longer entered in table T77UU. The report also enables you to delete the entries of the users no longer in the T77UU table from the INDX table.

You can use the RHBAUS02 report to enter users that have authorization for a large number of objects in table T77UU (*User Data in SAP Memory*) or to delete users with a small number of objects from this table.

This report enters users in the T77UU table or deletes users from this table if they have too small a number of objects depending on a threshold value. You can define the threshold value for the report (for example, 1000 for 1000 objects).

The report can then automatically perform the Customizing activity *Save User Data in SAP Memory*.

LESSON SUMMARY

You should now be able to:

- Outline the method to improve system performance for structural authorization profiles

Learning Assessment

1. Name the central elements of the Personnel Planning data model.

2. What advantages does the function module RH_GET_MANAGER_ASSIGNMENT offer in structural authorization?

3. What prerequisite must be fulfilled before you can assign structural authorizations to users using report RHPROFL0?

4. When should you generate indexes for structural authorizations?

Learning Assessment - Answers

1. Name the central elements of the Personnel Planning data model.

   The central elements are: Objects, relationships, and evaluation paths.

2. What advantages does the function module RH_GET_MANAGER_ASSIGNMENT offer in structural authorization?

   The function module determines the ID of the organizational unit headed by the manager. Thus, you can use one structural authorization for multiple managers.

3. What prerequisite must be fulfilled before you can assign structural authorizations to users using report RHPROFL0?

   You must first enter the structural authorization profiles in the PD Profiles infotype stored for the organizational unit, the job, the position, or the task.

4. When should you generate indexes for structural authorizations?

   You should generate indexes when you have structural authorizations containing a large number of objects.

UNIT 8 The Context Solution

Lesson 1

UNIT OBJECTIVES

- Outline issues related to the technical separation of general and structural authorization profiles
- Outline how using context authorization objects can solve authorization issues
- Generate context authorization objects

Unit 8
Lesson 1

Solving Context-Sensitive Authorizations

LESSON OVERVIEW

This lesson describes how to relate individual general and structural authorization profiles to each other to avoid unintentional overwriting of authorizations, and the potential issues arising when relating them. The lesson also describes how using context-sensitive authorizations can solve authorization issues.

Business Example

In your company, some managers are in charge of several departments. However, the managers' authorizations for accessing certain infotypes of the employees in their span of control should not be the same for all of those departments. You want to achieve this with the context solution. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Outline issues related to the technical separation of general and structural authorization profiles
- Outline how using context authorization objects can solve authorization issues
- Generate context authorization objects

Context Authorization Issues

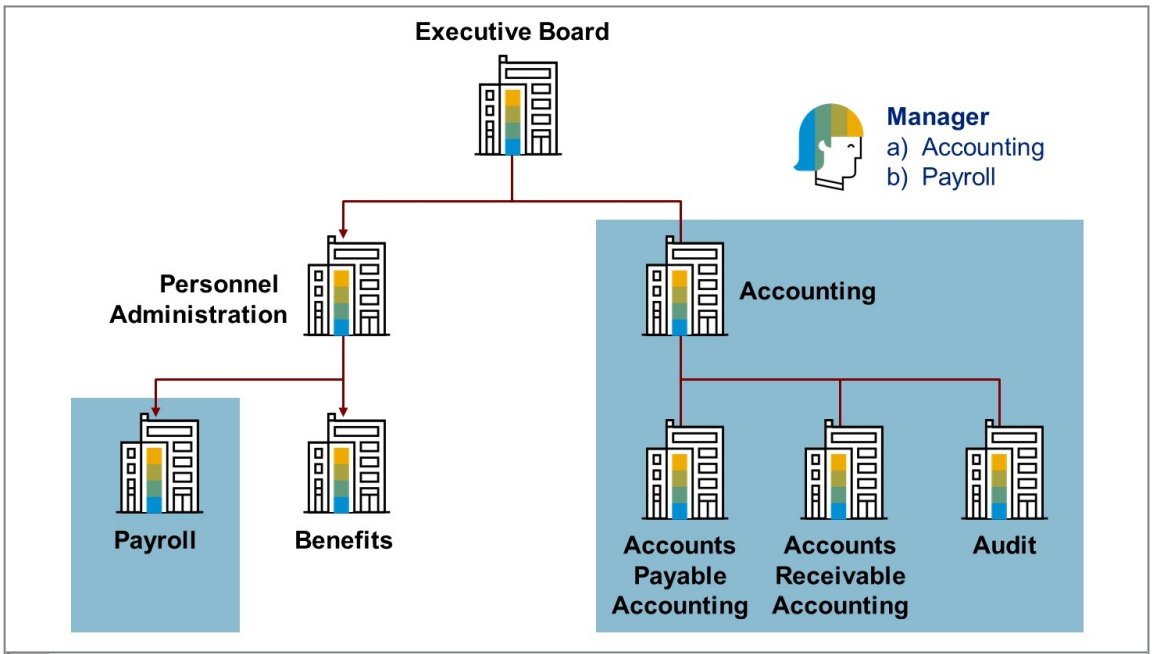

Figure 92: Context Problems in Human Resources (HR) Authorizations - Example 1

The technical separation of general and structural authorization profiles can cause context problems for users who perform different roles in a company. This is because you cannot simply add any number of structural and general authorization profiles required for different tasks in different contexts without overriding an authorization.

Consider a user who is a manager in the Accounting department. The user must be authorized to edit infotypes 0000 through 0007 of all the employees in the department. This user is also a manager for another organizational structure, Payroll. The user must have access to all payroll-relevant infotypes (0008 and 0015) for the employees in this organizational structure.

You cannot map the structural and general authorizations for such a user without the context solution because there is no relationship between a user's structural profile and basis authorization. The missing relationship leads to overriding.

Context Problems in HR Authorizations (2)

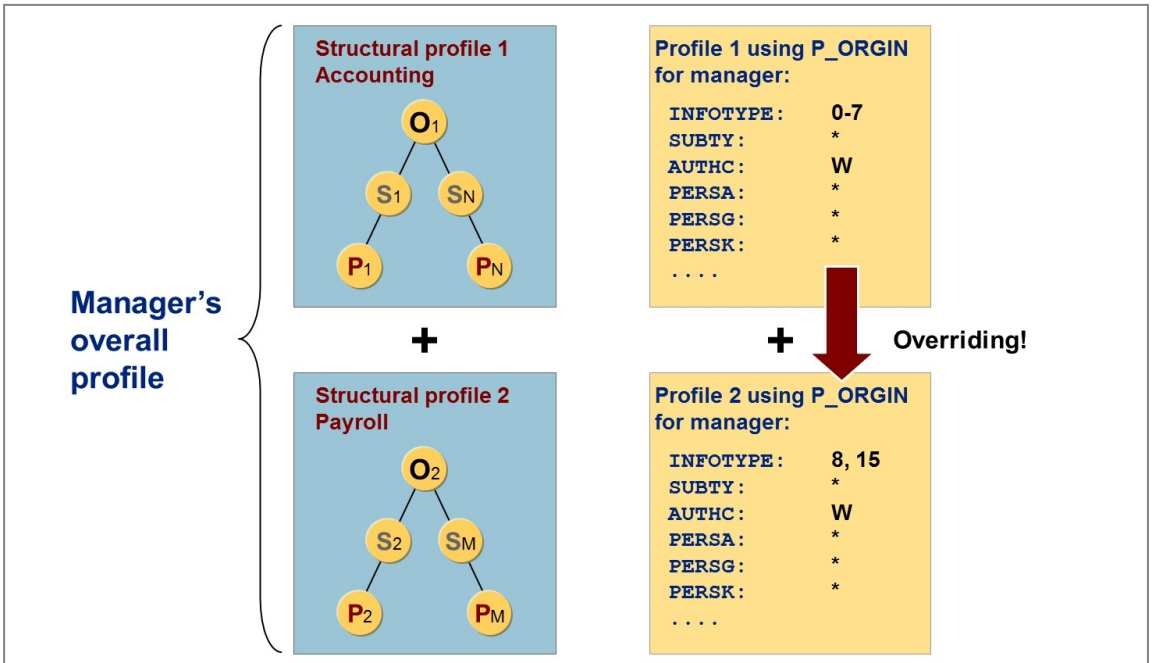

Figure 93: Context Problems in Human Resources (HR) Authorizations - Example 2

You cannot create an assignment between a user's specific structural profile (here, for example, structural profile 2) and a specific general profile (profile 2 with P_ORGIN).

The structural profiles (that is, the set of objects) and the general profiles (in this case, using P_ORGIN) are added to result in the overall profile. In the example shown in the figure, the manager has full read and write authorization for all objects from both the structural profiles.

When the authorization profiles are added, the following overall profile is produced:

- All employees in the manager's team and organizational structure
- Full read and write authorization for infotypes 0000 to 0008 and for 0015

If you use a separate user for each context, it is easier to map different contexts or roles with the correct authorizations. For example, if the manager wants to perform activities as an accounting manager, the manager uses manager's user name. If the manager wants to perform the role of a payroll manager, the manager uses a second system user with the respective authorizations.

You may need many users to map the user-specific contexts in your organization. Therefore, the context solution has been developed for HR master data.

The Context Authorization Solution

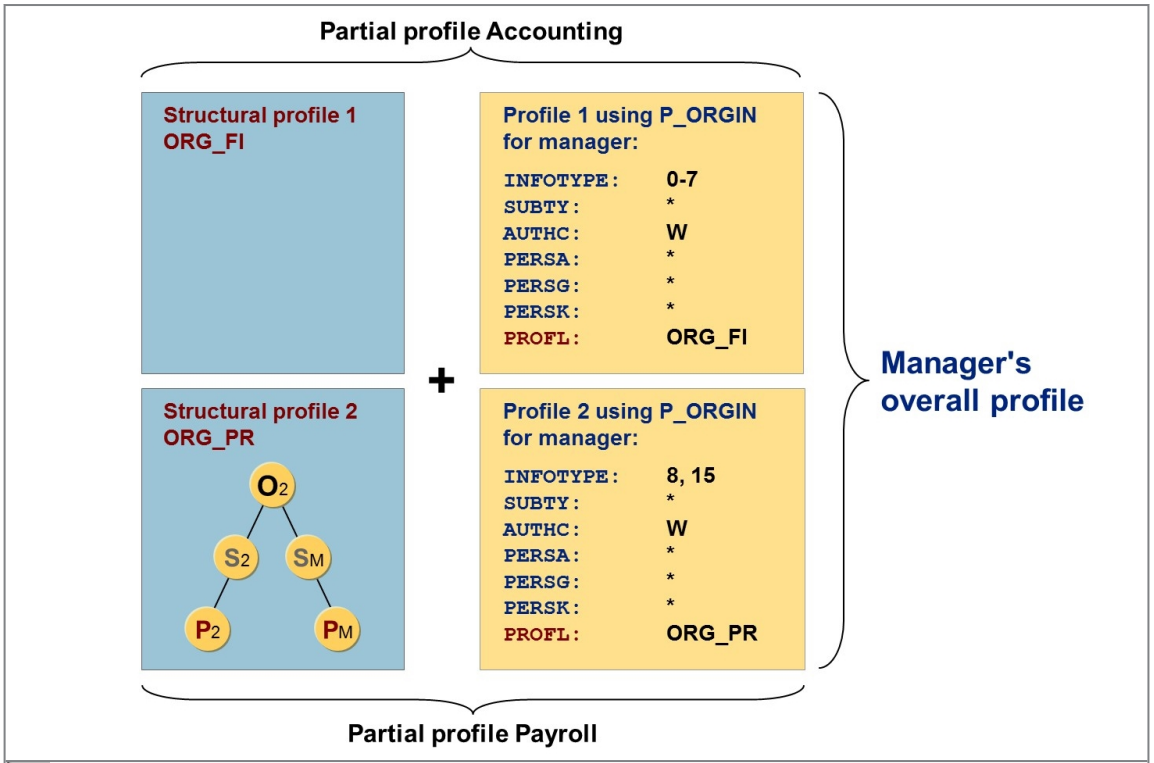

Figure 94: The Context Solution

The context solution is the context-sensitive realization of authorizations for HR master data. It enables you to do the following:

- Avoid overriding authorizations unintentionally.
- Relate individual general and structural authorization profiles to each other.

The context solution creates a technical connection between general and structural authorization profiles using special context-authorization objects. These context-authorization objects differ from the P_ORGIN and P_ORGXX authorization objects as they contain an additional field *PROFL*. You can enter structural profiles in this field.

Context Authorization Objects

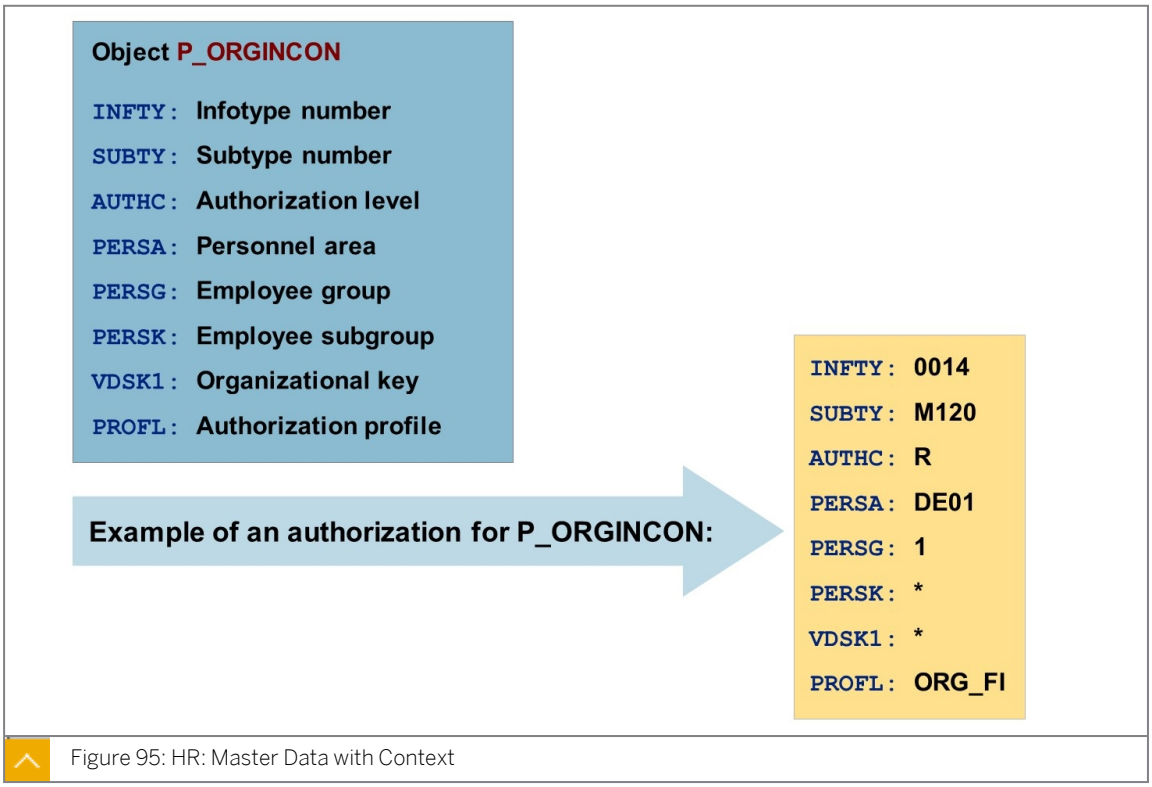

Figure 95: HR: Master Data with Context

The system uses the *HR: Master Data with Context* authorization object during the authorization check on HR infotypes. The check takes place when HR infotypes are edited or read. The system queries the contents of the fields during the authorization check.

You can use the authorization profile field, *PROFL*, to determine the structural profiles that a user is authorized to access.

In the standard system, the check of the *HR: Master Data with Context* authorization object is not active. You use the INCON authorization main switch to control the use of P_ORGINCON.

Hint:
The structural profiles assigned to a user are determined from the T77UA User Authorizations (Assignment of Profile to Users) table. Therefore, you must only use structural profiles that are entered in this table in the *PROFL* field of the context authorization objects.

HR: Extended Check with Context

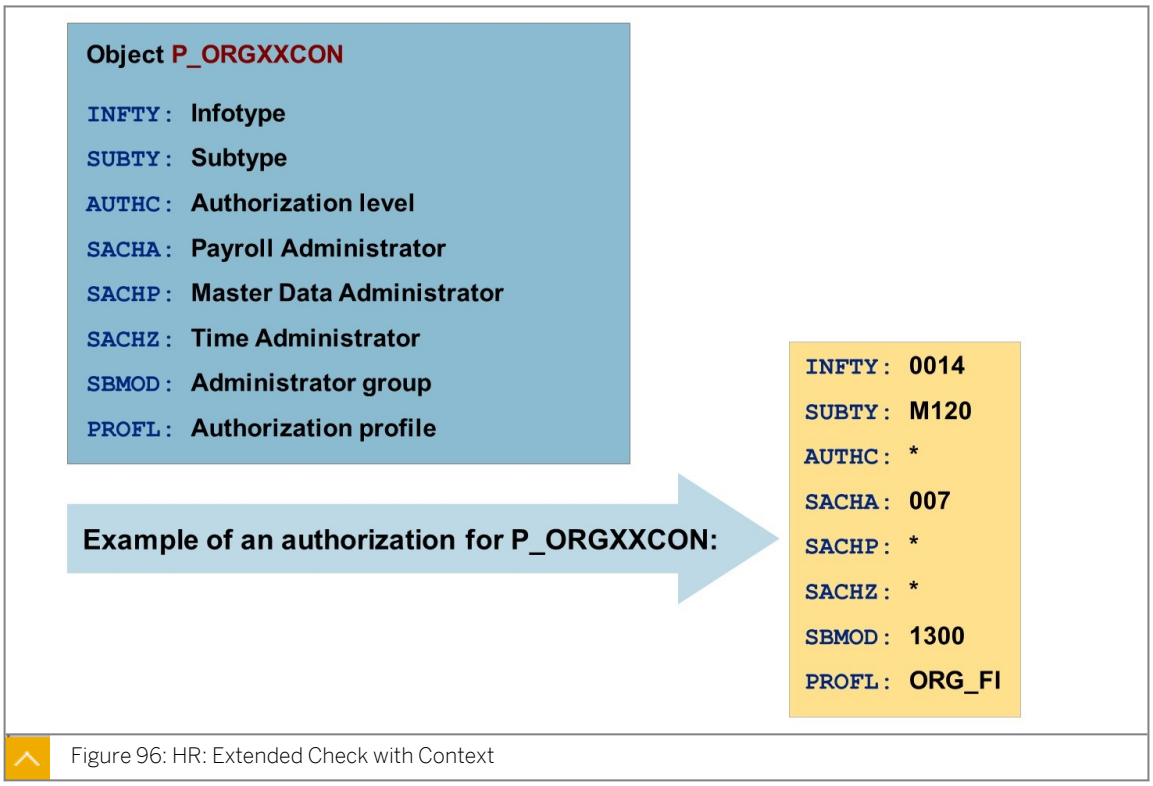

Figure 96: HR: Extended Check with Context

The system uses the *HR: Extended Check with Context* authorization object during the authorization check on HR infotypes. The check takes place when HR infotypes are edited or read.

The authorization profile field, *PROFL*, determines the structural profiles that the user is authorized to access.

In the standard system, *HR: Extended Check with Context* is not active. You use the XXCON authorization main switch to control the use of P_ORGXXCON.

Main Authorization Switches for the Context Solution

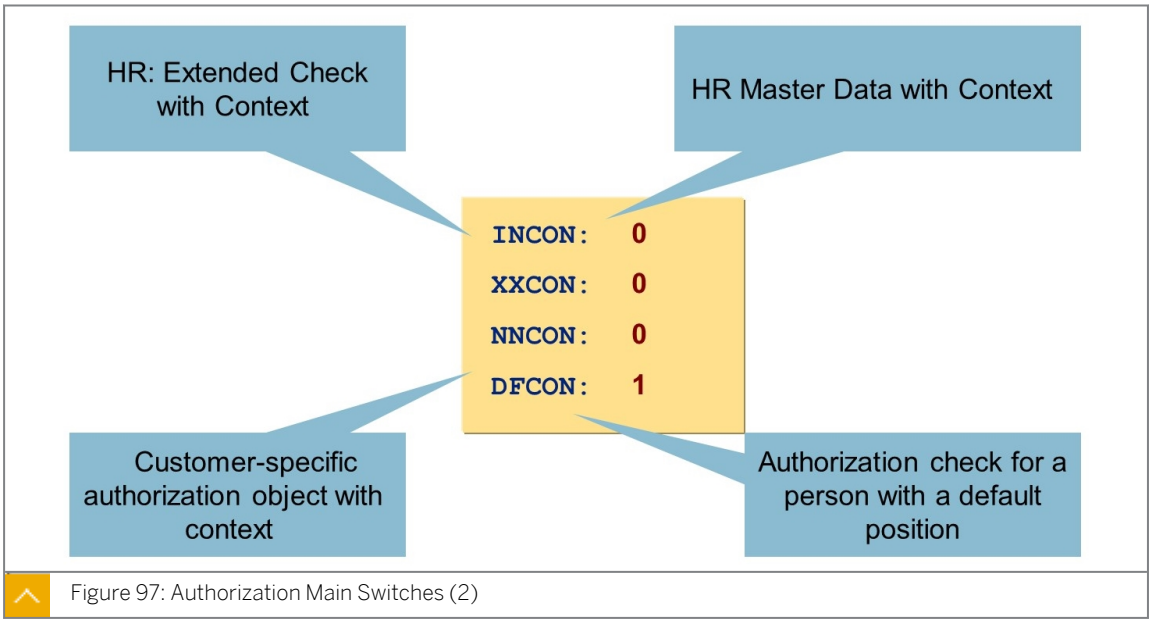

Figure 97: Authorization Main Switches (2)

The figure Authorization Main Switches shows the standard switch settings.

You can edit the standard switch settings using transaction OOAC or in Customizing for Personnel Administration under *Tools → Authorization Management → Edit Authorization Main Switch*.

Authorization Main Switches

INCON

This switch controls whether the HR: Master Data with Context object should be used in the authorization check.

XXCON

This switch controls whether the HR: Extended Check with Context object should be used in the authorization check.

NNCON

This switch controls whether a customer-specific authorization object with context should be used in the authorization check.

DFCON

This switch controls how the authorization check should be run for persons in the 99999999 default position.

Create Customer-Specific Object with Context

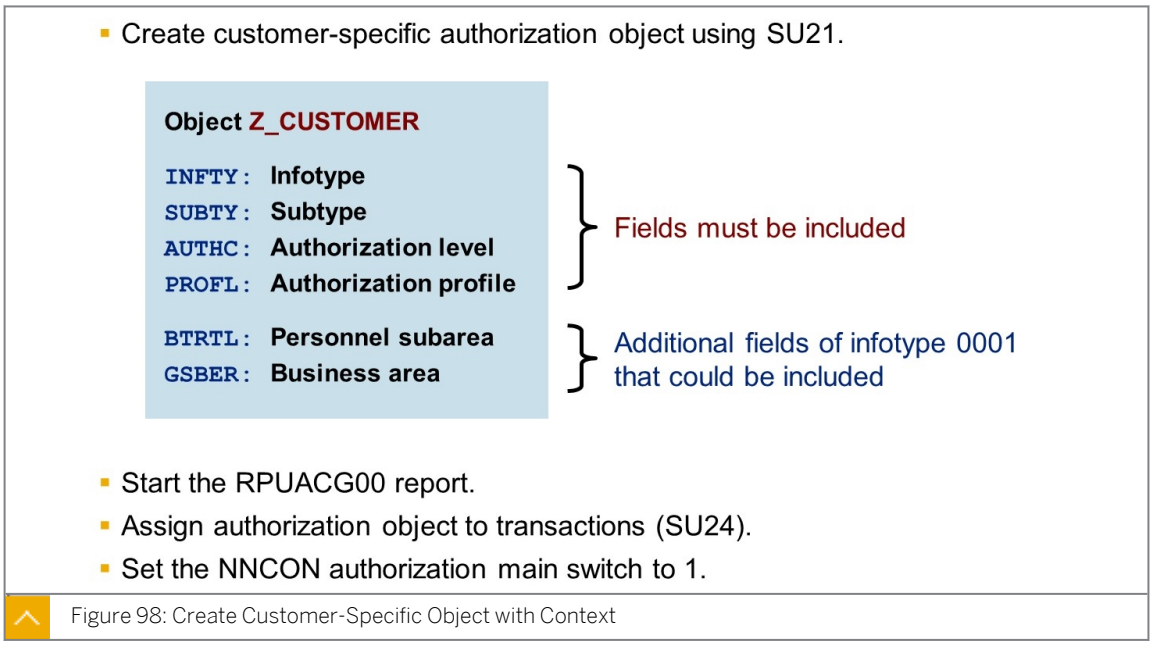

Figure 98: Create Customer-Specific Object with Context

Create the authorization object with transaction `SU21`, ensuring that you keep to the customer name range (Z/Y). To use the new authorization object you have created in the master data authorization check, the object must contain the *INFTY*, *SUBTY*, *AUTHC*, and *PROFL* fields.

The authorization profile field, *PROFL*, determines the structural profiles that the user is authorized to access.

In the standard system, the check of this object is not active. You can use the NNCON authorization main switch to control the use of your authorization object.

If you use customer-specific authorization objects, you must maintain these objects in transaction `SU24` (Maintain Assignment of Authorization Objects to Transactions) in the same way as you maintain the authorization objects P_ORGIN, P_ORGXX, and P_PERNR.

LESSON SUMMARY

You should now be able to:

- Outline issues related to the technical separation of general and structural authorization profiles
- Outline how using context authorization objects can solve authorization issues
- Generate context authorization objects

Learning Assessment

1. Which of the following statements correctly describes the addition of authorization profiles?

   Choose the correct answer.

   - ☐ **A** You can add up to two structural and general authorization profiles for different tasks in different contexts without overriding an authorization.
   - ☐ **B** You can add any number of structural and general authorization profiles for different tasks in different contexts without overriding an authorization.
   - ☐ **C** You can add any number of structural and general authorization profiles required for different tasks in different contexts by overriding some authorizations.
   - ☐ **D** You cannot add any number of structural and general authorization profiles required for different tasks in different contexts without overriding an authorization.

2. Which additional field does a context-sensitive authorization object have that P_ORGIN does not?

   Choose the correct answer.

   - ☐ **A** PERSG
   - ☐ **B** PROFL
   - ☐ **C** SUBTY
   - ☐ **D** AUTHC

Learning Assessment - Answers

1. Which of the following statements correctly describes the addition of authorization profiles?

   Choose the correct answer.

   - [ ] A You can add up to two structural and general authorization profiles for different tasks in different contexts without overriding an authorization.
   - [ ] B You can add any number of structural and general authorization profiles for different tasks in different contexts without overriding an authorization.
   - [ ] C You can add any number of structural and general authorization profiles required for different tasks in different contexts by overriding some authorizations.
   - [x] D You cannot add any number of structural and general authorization profiles required for different tasks in different contexts without overriding an authorization.

   Correct. You cannot add any number of structural and general authorization profiles required for different tasks in different contexts without overriding an authorization.

2. Which additional field does a context-sensitive authorization object have that P_ORGIN does not?

   Choose the correct answer.

   - [ ] A PERSG
   - [x] B PROFL
   - [ ] C SUBTY
   - [ ] D AUTHC

   Correct. The *PROFL* field has a context-sensitive authorization object, which P_ORGIN does not have.

UNIT 9

Additional Aspects of the General Authorization Check

Lesson 1

UNIT OBJECTIVES

- Outline authorization checks that use the organizational key
- Update an organizational key authorization

Unit 9
Lesson 1

Outlining Organizational Key Authorization Checks

LESSON OVERVIEW
This lesson outlines authorization checks that use the organizational key.

Business Example:

As the authorizations administrator, one of your tasks is to set up authorizations that use the organizational key. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Outline authorization checks that use the organizational key
- Update an organizational key authorization

Organizational Key

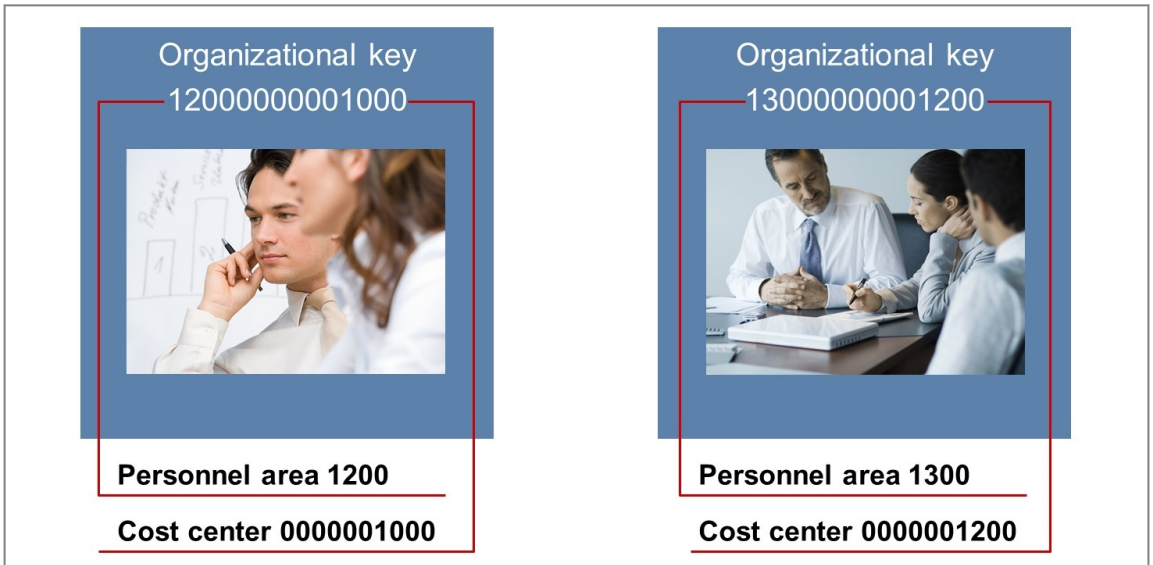

Figure 99: The Organizational Key

The organizational key (P0001-VDSK1 field) used to run differentiated authorization checks on the organizational assignment (using the P_ORGIN authorization object). The content of the organizational key is either derived by the system from the fields of the *Organizational Assignment* infotype (0001) or entered manually by the user.

The organizational key consists of a 14-character field in infotype 0001 that you can structure freely. You can use specific control and rule tables to help you structure the field. Do not confuse the organizational key with the organizational unit.

In the standard system, the organizational key is built up as follows: the first four places contain the personnel area and the following ten places contain the cost center.

You can create your own Organizational Key in configuration. The organizational key can be made up of any collection of field values found on Infotype 0001 and is limited to 14 character spaces.

The corresponding menu path in Customizing is *Personnel Management → Personnel Administration → Organizational Data → Organizational Assignment → Set Up Organizational Key*.

Organizational Key

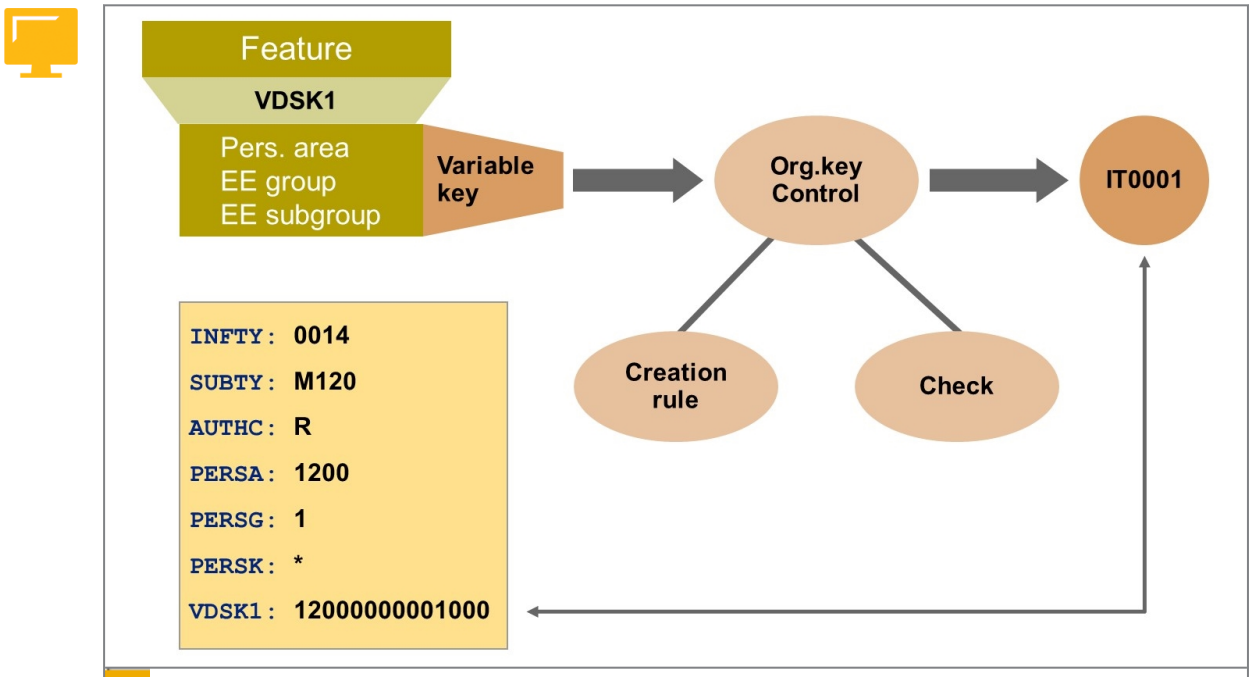

Figure 100: Organizational Key

The *Organizational Key* feature (VDSK1) and the T527 (*Organizational Key: Control*), T527A (*Organizational Key: Rules for Creating Organizational Keys*), and T527O (*Organizational Key: Validation*) tables control the creation and validation of the organizational key.

A variable key (VARKY) is determined for this purpose using the VDSK1 feature. This key is used according to table T527 to determine how the organizational key (VDSK1) should be created or validated.

The organizational key is stored in the Organizational Assignment infotype of the employee. When a user accesses the personnel data of the employee, the system checks whether authorization exists for the concrete value of the organizational key field.

In the example in the graphic, authorization exists for employees in personnel area 1200 who have been assigned cost center 1000.

Organizational Key Authorization

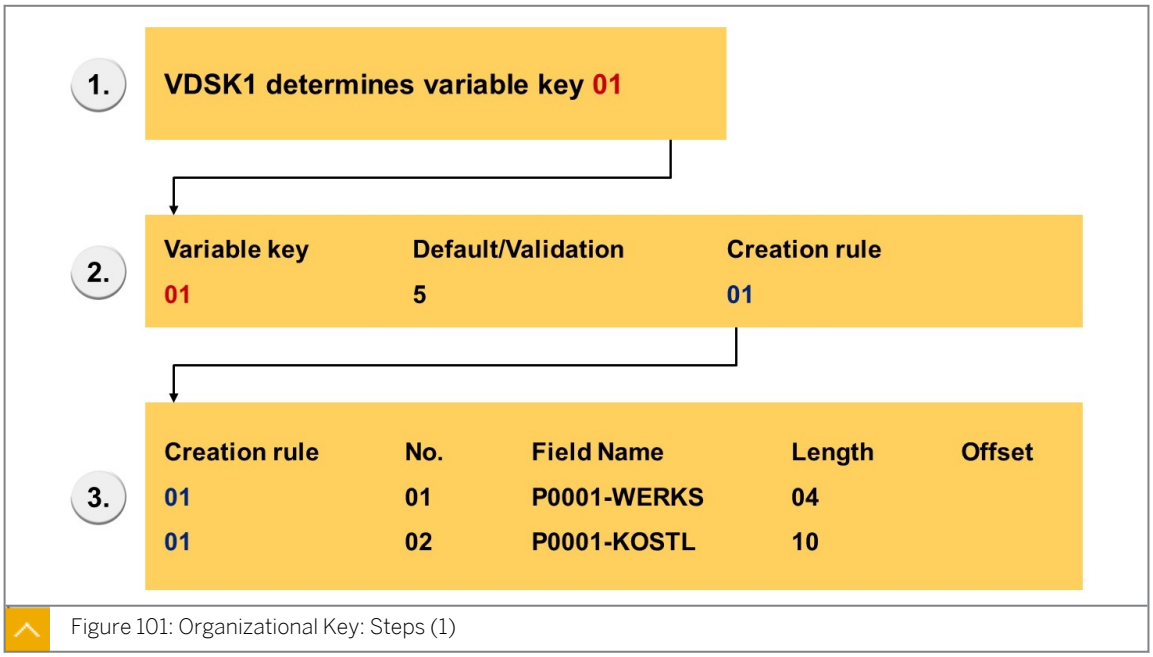

Figure 101: Organizational Key: Steps (1)

A variable key is determined using the VDSK1 feature.

This key is used according to the *Organizational Key: Control table* (T527) to determine how the organizational key should be created or validated. The fields *Default/Validation* and *Rule for Creating Organizational Keys* are evaluated for this purpose. The *Default/Validation* field can contain the following values:

1 = optional entry without validation

2 = optional entry with validation

3 = required entry with validation

4 = default that cannot be overwritten without validation

5 = default that can be overwritten without validation

6 = default that can be overwritten with validation

7 = default that cannot be overwritten with validation

If you make an entry for *Default/Validation* which causes a default value to be created (entries 4, 5, 6 or 7), you must also maintain the *Rule for Creating Organizational Key* field. This entry is then used to determine the corresponding creation rule for the organizational key *Organizational Key: Rule for Creating Organizational Key* table (T527A).

If you make an entry for *Default/Validation* which causes the organizational key to be validated, you must enter the values that should be recognized by the system as permitted in the *Organizational Key Validation* table (T527O).

Organizational Key: Steps (2)

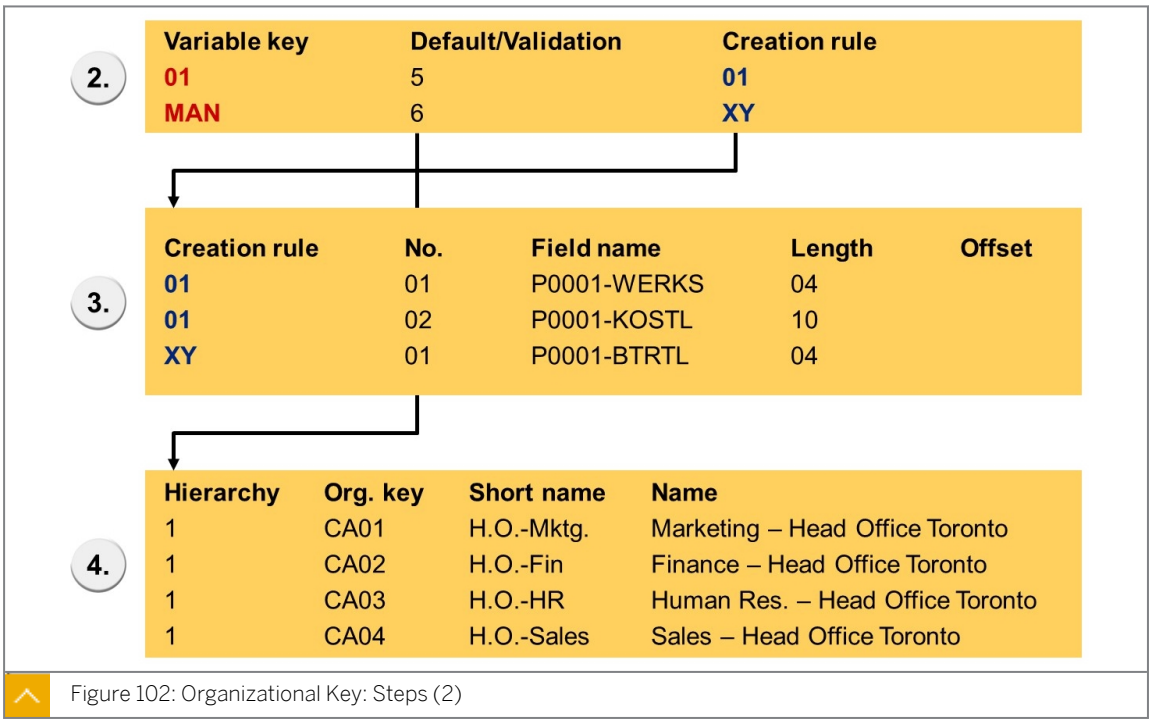

Figure 102: Organizational Key: Steps (2)

If you make an entry for *Default/Validation* which causes the organizational key to be validated, you must enter the values that should be recognized by the system as permitted in the *Organizational Key Validation* table (T527O).

The *Organizational Key: Validation* table contains a list of the permitted entries for the *Organizational Key* field (VDSK1). Only entries with *hierarchy* = 1 are relevant for validation. All other entries are ignored when validating the organizational key.

The *Organizational Key* column contains the organizational key that should be permitted during the validation.

In the *Short Name* and *Name* columns, you can store a short text or a description for each organizational key. The texts appear when you call input help for the *Organizational Key* field. The texts are irrelevant for the actual validations.

LESSON SUMMARY

You should now be able to:

- Outline authorization checks that use the organizational key
- Update an organizational key authorization

Learning Assessment

1. What is the function of the organization key in the Organizational Assignment infotype?

Learning Assessment - Answers

1. What is the function of the organization key in the Organizational Assignment infotype?

   The organization key enables you to use differentiated authorization checks for the authorization object HR: Master Data.

UNIT 10 HR Authorization: Optimization

Lesson 1

UNIT OBJECTIVES

- Evaluate HR authorization profiles
- Outline the setup for employee views of data in ESS
- Restrict the maintenance of user data by the user
- Outline the use of checks based on infotype subtypes
- Outline the setup of authorizations for batch input sessions
- Recognize the redundant read of objects
- Outline customer enhancements available using business add-ins (BAdIs)

Unit 10
Lesson 1

Optimizing HR Authorizations

LESSON OVERVIEW
This lesson outlines options you can use to optimize HR authorizations.

Business Example:

You are responsible for HR authorizations and want to optimize how HR authorizations are handled by the SAP system. For this reason, you require the knowledge provided in this lesson.

LESSON OBJECTIVES
After completing this lesson, you will be able to:

- Evaluate HR authorization profiles
- Outline the setup for employee views of data in ESS
- Restrict the maintenance of user data by the user
- Outline the use of checks based on infotype subtypes
- Outline the setup of authorizations for batch input sessions
- Recognize the redundant read of objects
- Outline customer enhancements available using business add-ins (BAdIs)

HR Authorization Workbench

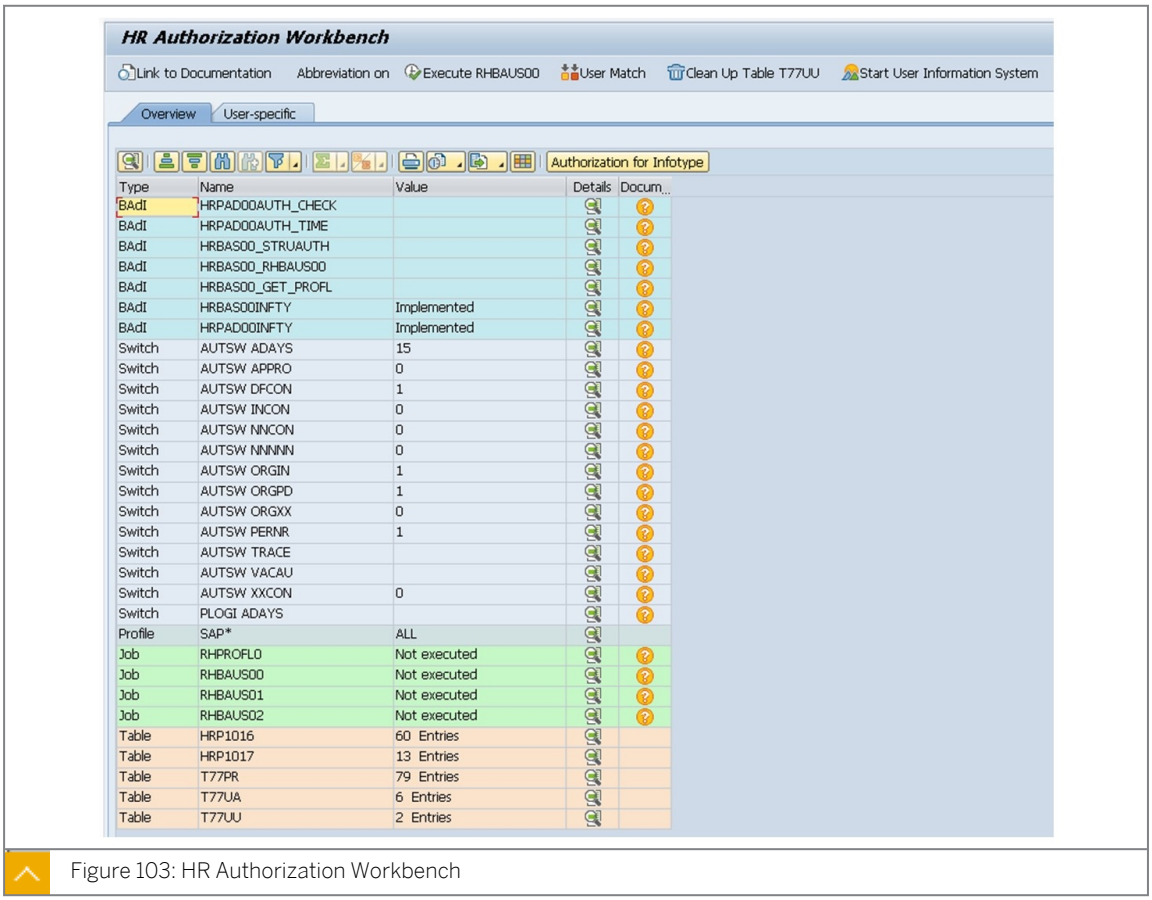

Figure 103: HR Authorization Workbench

Transaction HRAUTH enables you to evaluate the HR authorization profiles that exist for a user. This includes the structural authorization profiles as well as the HR Basis authorization profiles that are assigned to the user directly (using role maintenance) or indirectly (in Organizational Management).

In the HR Authorization Workbench, you can access several functions that enable selective evaluation of the authorization profiles. You can display the following information among other things:

- The complete list of authorization main switches with the values set for them (in the function bar on the selection screen).
- All of the persons assigned to the user in the *Communication*infotype (0105) (in the function bar on the selection screen).
- The organizational units with which the user is related.
- The structural authorization profiles.
- The user's role assignments and standard profiles.
- The authorizations based on HR authorization objects (of Personnel Administration/ Personnel Planning - multiple selection is possible).

Employee Self-Service

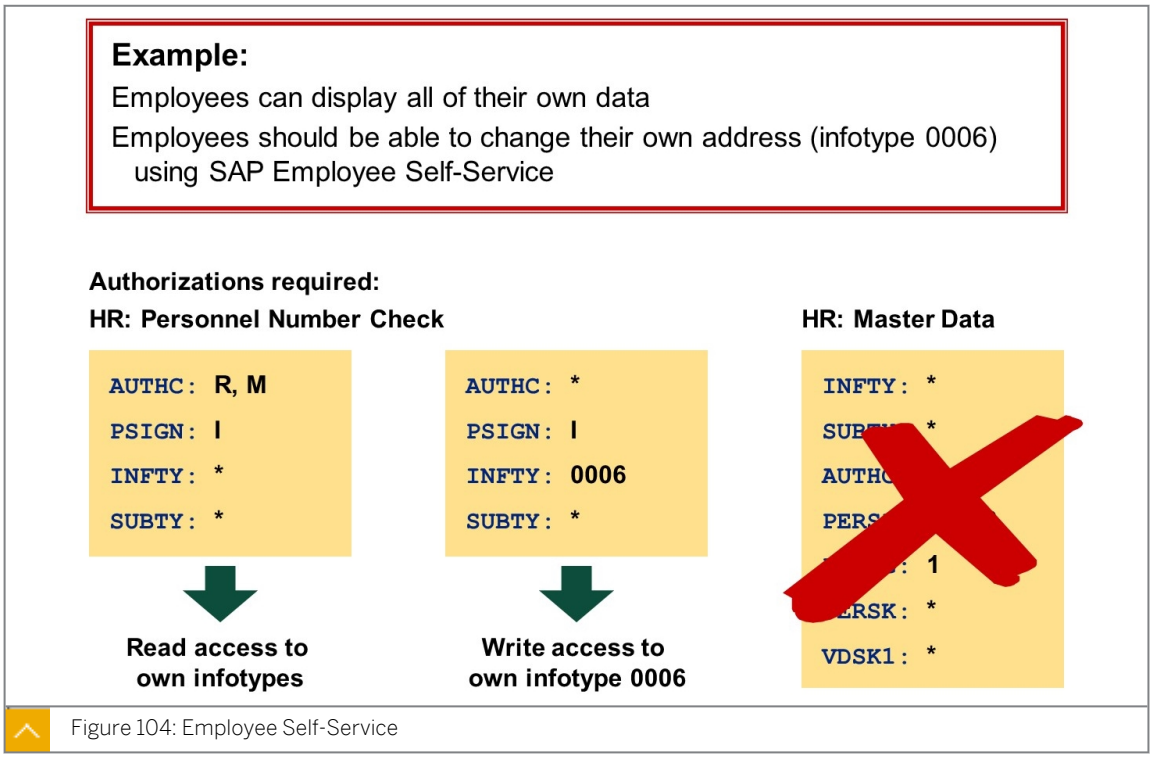

Figure 104: Employee Self-Service

Prerequisites: The AUTSW PERNR main switch must be activated to enable the authorization check by personnel number.

The user assignment for all employees who use the SAP Employee Self-Service must be maintained in infotype 0105.

Users who are not administrators should not be granted P_ORGIN authorizations.

Every employee who uses the SAP Employee Self-Service is granted the two authorizations mentioned above for the P_PERNR authorization object: The first authorization grants the employee read authorization for all infotypes that are stored under the employee's personnel number. The second authorization grants write authorization for all data records of the 0006 infotype of the employee's own personnel number.

Data Maintenance

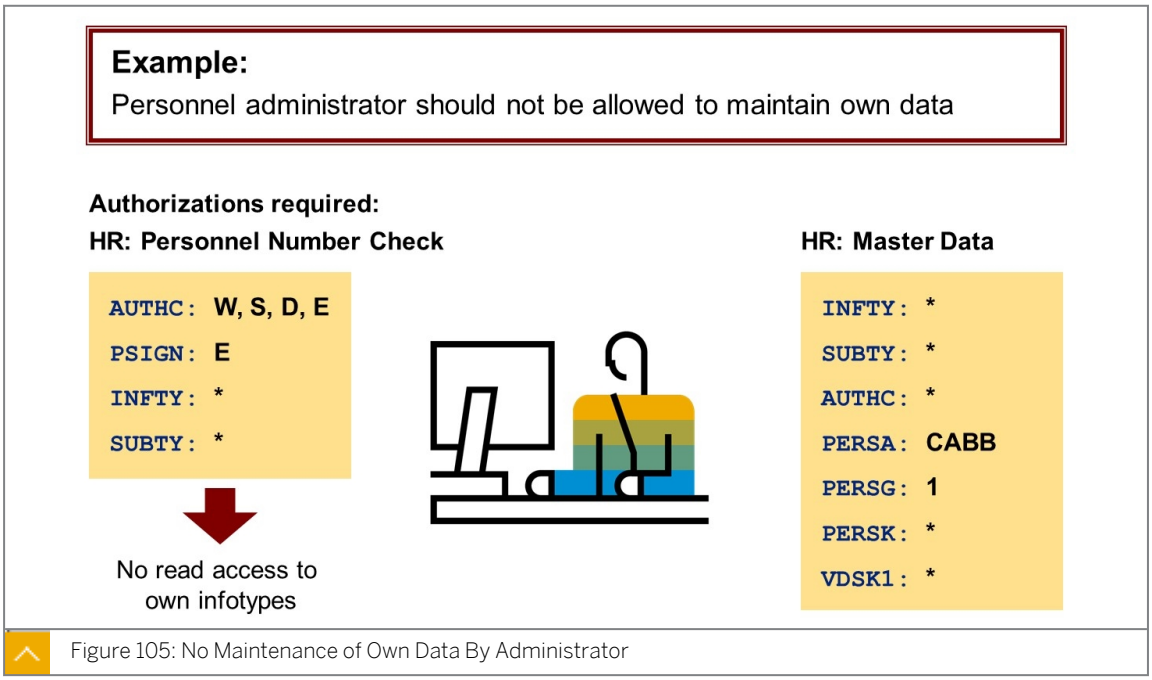

Figure 105: No Maintenance of Own Data By Administrator

Prerequisites:

The AUTSW PERNR main switch must be activated to enable the authorization check by personnel number.

The user assignment for the corresponding administrator must be maintained in infotype 0105.

Each employee affected is granted the P_PERNR authorization shown in the figure No Maintenance of Own Data By Administrator.

Authorizations for an Infotype Subtype Check

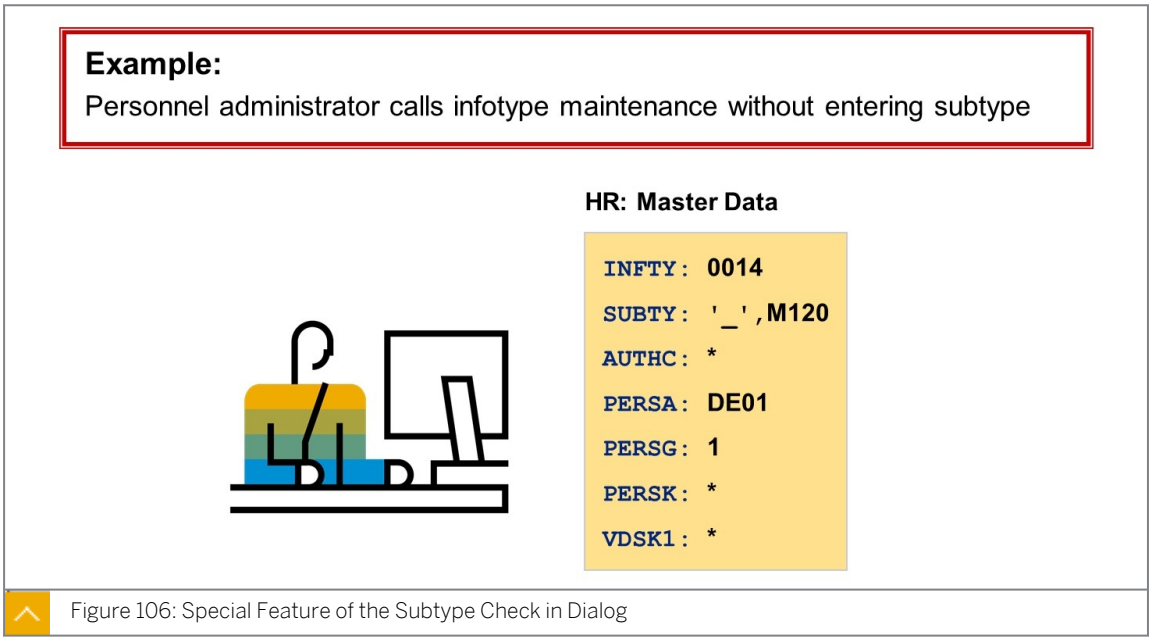

Figure 106: Special Feature of the Subtype Check in Dialog

Problem:

For certain infotypes (such as 0014, 0015, and 2010), you can create a new record without having to specify a subtype on initial access to the individual record maintenance. If an administrator wants to create a new record without specifying a subtype, the authorization check consequently takes place using the subtype <BLANK>. This often results in users with limited subtype authorizations not being able to access the infotype screen. There are two ways to avoid this:

1. Users always explicitly specify a subtype for which they have authorization.
2. Users are granted an additional authorization for the dummy subtype <BLANK>.

Hint:
Solution 2 is preferred. In principle, users are not granted any unnecessary authorizations by this, since the <BLANK> subtype does not exist and is always explicitly checked when users access existing data records and when they create new data records.

Authorizations for Batch Input Sessions

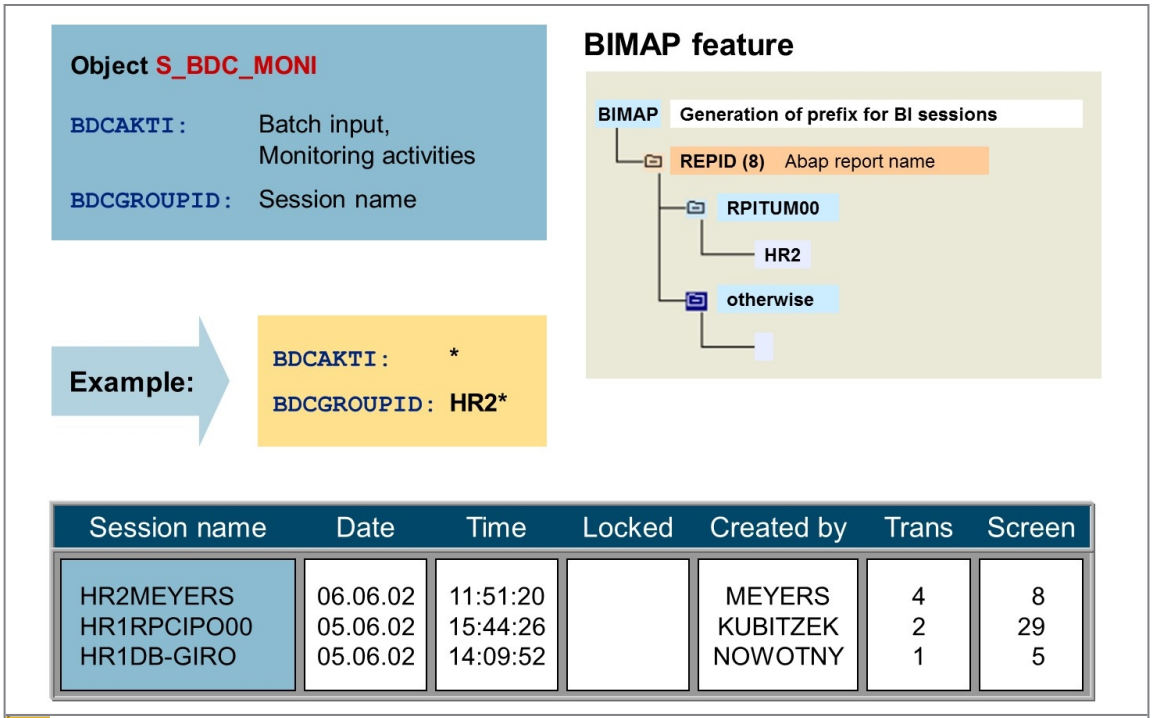

Figure 107: Authorizations for Batch Input Sessions

You can define report-specific prefixes to protect batch input sessions. The prefix is set before the actual session name and can be checked generically later. This ensures that sessions are not processed without authorization.

Using the object *Batch Input Authorizations* (technical name: S_BDC_MONI) in the object class Basis Administration, you can create authorizations based on the session name and actions, for example, processing a batch input session or displaying a processing log.

You can define report-specific prefixes using the BIMAP feature to protect batch input sessions. The prefix is set before the actual session name and is then checked generically by the *Batch Input Authorizations* object. Example: The session name MEYERS becomes HR2MEYERS if a corresponding entry exists in the feature.

In the example shown in the figure Authorizations for Batch Input Sessions, the system proposes the HR2 prefix for the session name of the RPITUM00 program. All other programs do not use a prefix.

Hint:
The BIMAP feature is delivered by SAP with an empty decision tree.

Redundant Read of Objects

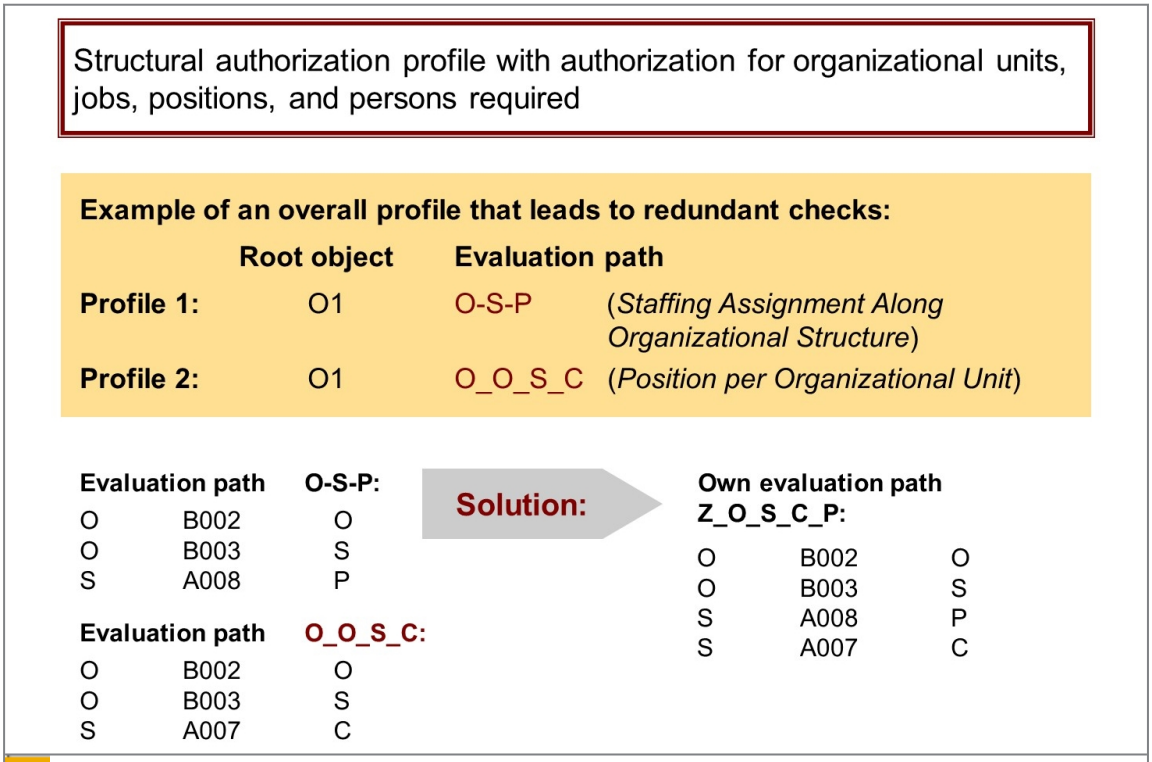

Figure 108: Redundant Read of Objects

To avoid unnecessary loss of performance, ensure that there are as few redundancies as possible when you define structural authorizations. In other words, the entries for a user in table T77PR should not overlap if possible (refer to the figure Redundant Read of Objects). This type of profile (several evaluation paths used) is often used to implement authorization requirements that cannot be met using a standard evaluation path.

In the present example, the profile needs to contain authorization for organizational units, jobs, positions, and persons. This combination is not covered by any standard evaluation path, which is why the two evaluation paths in the graphic are used.

However, this can lengthen the creation of the set of objects for the structural authorization because specific objects (O, S) are read several times. If the O-S-P and O_O_S_P evaluation paths are used simultaneously, organizational units (O) and positions (S) are read redundantly during the creation of the set of objects.

Proposed Solution:

You can avoid this if you define your own evaluation path that meets all the requirements of the authorization profile and reads the necessary objects only once. In the example used here, you could define a Z_O_S_C_P evaluation path, for instance.

Customer Enhancements Using BAdIs

If your requirements of the authorization check for HR Master Data infotypes cannot be met by either the standard system or by a customer-specific authorization object, you can replace the authorization checks completely without modification (as of Release 4.6C). For this, you use Business Add-Ins (BAdI).

HRPAD00AUTH_CHECK (HR: Authorization Check)

HRBAS00_STRUAUTH (Structural Authorization)

HRBAS00_GET_PROFL (Define Assigned Structural Profiles)

Figure 109: Customer Enhancements Using BAdIs

You can find the BAdI **HRPAD00AUTH_CHECK** in the Implementation Guide (IMG) for Personnel Management under *Personnel Administration → Tools → Authorization Management → BAdI: Set Up Customer-Specific Authorization Check*. You can find information on implementing a BAdI in the documentation of the corresponding IMG activity. As soon as an implementation for this BAdI is active, **all** HR master data authorization checks of the standard system are stopped, and instead only the activated implementation is performed.

As for general authorization checks, you can also implement a customer-specific test procedure for the structural authorization check using a BAdI. You can find the Business Add-In **HRBAS00_STRUAUTH** in the IMG for *Personnel Management* under *Organizational Management → Basic Settings → Authorization Management → Structural Authorization → BAdI: Structural Authorization*. You can find information on implementing a BAdI in the activity documentation.

The BAdI **HRBAS00_GET_PROFL** is of particular interest if you implement the context solution: It means that you do not need to maintain table T77UA (*User Authorizations*). You find the BAdI in the Implementation Guide (IMG) for *Personnel Management* under *Organizational Management → Basic Settings → Authorization Management → Structural Authorization → BAdI: Define Assigned Structural Profiles*. You can find information on implementing a BAdI in the documentation of the corresponding IMG activity.

LESSON SUMMARY

You should now be able to:

- Evaluate HR authorization profiles
- Outline the setup for employee views of data in ESS
- Restrict the maintenance of user data by the user
- Outline the use of checks based on infotype subtypes
- Outline the setup of authorizations for batch input sessions
- Recognize the redundant read of objects

- Outline customer enhancements available using business add-ins (BAdIs)

Learning Assessment

1. Employees that use Employee Self-Service require authorization for the authorization object HR: Master data.

   Determine whether this statement is true or false.

   ☐ True

   ☐ False

2. In an authorization, if you list individual subtypes in the Subtype field, you should also enter the subtype Blank. What is the reason for this?

   _____

   _____

   _____

Learning Assessment - Answers

1. Employees that use Employee Self-Service require authorization for the authorization object HR: Master data.

   Determine whether this statement is true or false.

   ☐ True

   ☒ False

   Correct. Employees that use Employee Self-Service may only have authorization for the authorization object HR: Master data - personnel number check.

2. In an authorization, if you list individual subtypes in the Subtype field, you should also enter the subtype Blank. What is the reason for this?

   With certain infotypes, it is possible to create a new record without having to specify a subtype in the Subtype field when you access individual record maintenance. If the dummy subtype Blank is not stored in the user's authorization, the user must always specify a subtype for which he or she has authorization.